SHEPPARD, MULLIN, RICHTER & HAMPTON LLP
Rena Andoh (admitted *pro hac vice*)
randoh@sheppardmullin.com.com
30 Rockefeller Plaza
New York, NY 10112
Telephone: (212) 653-8700
Facsimile: (212) 653-8701

Lai L. Yip (SBN 258029)
lyip@sheppardmullin.com
Four Embarcadero Center, 17th Floor
San Francisco, CA 94111
Telephone: (415) 434-9100
Facsimile: (415) 434-3947

Travis J. Anderson (SBN 265540)
tanderson@sheppardmullin.com
12275 El Camino Real, Suite 100
San Diego, CA 92130
Telephone: (858) 720-8900
Facsimile: (858) 509-3691

Kazim A. Naqvi (SBN 300438)
knaqvi@sheppardmullin.com
1901 Avenue of the Stars, Suite 1600
Los Angeles, CA 90067
Telephone: (310) 228-3700
Facsimile: (310) 228-3701

Attorney for Plaintiff and Counter-Defendant Moog Inc.

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

MOOG INC.,

Plaintiff,

v.

SKYRYSE, INC., ROBERT ALIN PILKINGTON, MISOOK KIM, and DOES NOS. 1-50,

Defendants.

Case No. 2:22-cv-09094-GW-MAR

MOOG INC.'S AMENDED COMPLAINT

Complaint Filed: March 7, 2022
Counterclaims Filed: January 30, 2023

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

Judge: Hon. George H. Wu

SKYRYSE, INC.,

Counterclaimant,

vs.

MOOG INC.,

Counter-Defendant

Plaintiff Moog Inc. ("Plaintiff" or "Moog"), by and through its undersigned counsel, Sheppard, Mullin, Richter & Hampton LLP, for its Amended Complaint, alleges against Defendants Skyryse, Inc. ("Skyryse"), Robert Alin Pilkington ("Pilkington"), Misook Kim ("Kim"), and DOES Nos. 1-50 (collectively, "Defendants") as follows. The allegations herein are made based on personal knowledge as to employees of Plaintiff, and its own actions and interactions, and upon information and belief as to all other matters.

NATURE OF THE ACTION

1. Moog commenced this action on March 7, 2022 to stop: 1) the illegal taking and use of its trade secrets and the misappropriation of sensitive US government technical data developed by Moog; and 2) the raiding of Moog employees to exploit such information and unfairly compete. At the time the initial Complaint was filed, Moog had discovered that prior to leaving Moog to join Skyryse, defendant Misook Kim had stolen over 136,000 files of Moog's most sensitive and proprietary data relating to its flight control software (including over 43,000 source code files) that has taken over 16 years to develop. Since the filing of the Complaint, Moog has discovered additional acts of theft and misappropriation by current and former Skyryse personnel, including a separate massive theft of files by former Moog employee Alin Pilkington – who also departed for Skyryse immediately after his theft – such that the volume of stolen data ***exceeds 1.4 million files*** related to five comprehensive and foundational toolsets, 21 flight control programs (including several sensitive government programs), and other categories of information. The extent of misappropriation and theft in this case, as confirmed by forensic analysis and discovery, is staggering.

2. The underlying history between Moog and Skyryse is telling. Founded in 1951, Moog is a publicly traded (NYSE: MOG.A, MOG.B) aerospace and defense company, with annual sales of approximately $3 Billion and a world-wide workforce of over 13,000. Moog has developed and supplies the flight control

systems for some of the most common commercial and military aircrafts used today. Moog has been pursuing autonomous flight projects, including with Robinson R-44 aircrafts, since 2012.

3. Skyryse is a venture-backed tech aviation start-up company founded by CEO Mark Groden in 2016. Moog and Skyryse began a business relationship in 2018, and entered into multiple NDAs to share limited proprietary information with each other. At the time, Skyryse pitched its business as a "commuter service" to provide an Uber-of-the-skies type of business. It did not convey any intention of developing its own autonomous flight systems. During these initial discussions, Moog would provide the helicopter flight control systems, and Skyryse would install and implement this technology into its business plan to offer public autonomous helicopter transportation. The parties worked together until December 2019, when Skyryse announced it was offering autonomous flight as part of its own flight control operating system it was developing (called FlightOS). Skyryse subsequently elected to cancel the Parties' underlying statement of work, all while it was pivoting to a core Moog business (flight control software development). In an RFQ in May of 2020, Skyryse requested that Moog agree to perform large portions of the work associated with this pivot. But Skyryse did not want to pay Moog the amount required for Moog to conduct that work and the Parties' relationship ended.

4. Skyryse then raised $200 million in Series B fundraising culminating on October 27, 2021. Over the next six months, Skyryse engaged in a targeted campaign to poach at least 20 former Moog employees, including key Moog personnel with intimate knowledge of Moog's flight control software and other proprietary data. Moog discovered that on November 19, 2021, one week after her manager Pilkington's departure, Kim copied onto an external hard drive 136,994 proprietary Moog files consisting of nearly all source code, documentation, and planning documents related to at least 12 Moog programs (including several sensitive military programs). Kim also specifically copied Pilkington's Moog files

(i.e., Pilkington's "branch" of work in Moog's source code repository). When Moog later demanded that Kim return the hard drives used in the data theft, Kim returned two separate hard drives, both of which had been completely wiped clean. Forensic analysis confirmed that Kim attempted to cover her tracks by re-naming one device to mimic a different device, using yet another electronic device to steal Moog data, and deleting its contents such that they were unrecoverable from that device.

5. As Moog's internal investigation continued after the filing of the Complaint, and as it engaged in expedited discovery in this case, Moog has since discovered that ***Pilkington himself copied over 1.2 million Moog files upon his departure to Skyryse***, including virtually all source code, documentation, and planning documents from 5 Moog toolsets and 21 Moog programs. Kim and Pilkington's theft of Moog data is undisputed, and they have confirmed as much in written discovery responses. Moog has also discovered that several Skyryse personnel other than Kim and Pilkington were involved in the possession, transfer, and/or use of Moog trade secrets and other proprietary information, and disclosed such trade secrets and proprietary information to third parties. Moog has also discovered voluminous examples of Skyryse directly copying Moog's software-related documents, including by directly using and copying Moog's software checklists and templates, and modeling Skyryse's software development and verification plans off of Moog's documents. It is not a coincidence that these stolen files are directly related to the very work that Skyryse asked Moog to bid for, but did not want to pay Moog to do.

6. Moog now brings causes of action for breach of contract, breach of the implied covenant of good faith and fair dealing, misappropriation of trade secrets pursuant to the federal Defend Trade Secrets Act, conversion, breach of fiduciary duty, aiding and abetting breach of fiduciary duty, conspiracy, unjust enrichment, and violation of California's unfair competition law arising out of Skyryse's and the individual defendants' egregious and ongoing acts of contractual violations,

intellectual property misappropriation and theft, and corporate raiding.

7. These causes of action seek to redress a coordinated scheme by Defendants to misappropriate valuable confidential, proprietary, and trade secret information by way of stealing it, and further recruit swaths of Moog's valuable employees to use that misappropriated information to improperly shortcut Skyryse's own research and development costs and timeline to give Skyryse a competitive advantage, and undercut, steal, and/or interfere with Moog's business. The information stolen by Defendants from Moog, which includes the source code of highly proprietary software programs that are critical to Moog's ability to provide services to its many commercial and government customers, is the result of years of work and many millions of dollars invested by Moog. Defendants' improper use of this confidential and sensitive information, if not stopped, will lead to irreparable harm to Moog, give a competitor an extreme and unfair advantage in a highly competitive emerging market, and severely impact both Moog's current and future business.

8. Further, the Defendants' targeted, improper, and ongoing raiding of Moog's software engineering force, which has resulted in a loss of dozens of critical developers and engineers, presents substantial disruption and jeopardy to Moog's ongoing business. Skyryse is unfairly competing by simultaneously crippling Moog's staffing numbers through wrongful means while having former Moog employees utilize and build on Moog's confidential, proprietary, and trade secret information for Skyryse's benefit.

9. If Defendants are not stopped, they will continue to more completely integrate, utilize, and improperly trade upon decades' worth of misappropriated information belonging to Moog in an attempt to beat Moog and several other competitors in the unmanned aircraft market, and will continue to methodically and increasingly plunder Moog's employees in an effort to unfairly shortcut Skyryse's own development process. In doing so, Defendants will continue to irreparably harm

Moog.

10. Moog seeks injunctive relief to address irreparable harm and to recover damages arising from Defendants' unlawful conduct. Defendants' conduct was and continues to be willful and malicious. Moog further seeks injunctive relief to prevent Defendants from fully consummating their scheme to take Moog's business and/or improperly augment and accelerate Skyryse's business through improper use of the misappropriated information and expanded hiring of Moog's employees for the relevant business.

THE PARTIES

11. Founded in 1951 in East Aurora, New York, Moog is a publicly traded (NYSE: MOG.A, MOG.B) aerospace and defense company. It has annual sales of approximately $3 billion and a world-wide workforce of over 13,000. Moog is a designer and manufacturer of electric, electro-hydraulic and hydraulic motion, controls and systems for applications in aerospace, defense, industrial and medical devices. The company operates under three segments: aircraft controls, space and defense controls, and industrial controls. Moog has developed and supplies the flight control systems for some of the most common commercial aircrafts used today, including the Boeing 787, Airbus A350, Embraer E2 regional jet and multiple business jets for Gulfstream and others. Moog has also developed and supplies the flight control systems for some of the most common military aircrafts used today, such as the F15, F18, and F35 fighter aircrafts. It has also developed systems and components for some of the most critical commercial and government sponsored space and defense systems, including the International Space Station, United Launch Alliance, Apollo and Artemis missions, James Web and Hubble Telescopes, and the Perseverance and Mars Lander projects. Moog works frequently on sensitive United States government projects, as well as third-party commercial projects. Moog has sales, engineering, and manufacturing facilities in twenty-six countries. Moog is a New York corporation. Moog's corporate headquarters are located at 400 Jamison

Road, East Aurora, New York. Moog maintains offices at 20263 S. Western Avenue, Torrance, CA 90501.

12. Defendant Skyryse, Inc. is a Delaware corporation with its principal place of business at 777 Aviation Blvd, El Segundo, California. Skyryse is a venture-backed tech aviation start-up company founded by CEO Mark Groden in 2016. Skyryse is privately held and Moog is unaware of its annual sales. Skyryse's stated goal is to build autonomous flying aircraft, *i.e.*, aircraft without pilots, and to build such autonomous flying systems into already-developed aircraft. Skyryse had an initial venture capital funding of $25 million and announced in October 2021 another $200 million investment by various venture capital firms. Skyryse's total employment is unknown to Moog, but the current employees of Skyryse hired from Moog are believed to have formed a significant portion of Skyryse's technical workforce.

13. Defendant Robert Alin Pilkington is a resident of the State of California. Pilkington was employed by Moog from on or about July 30, 2012 to November 12, 2021. At the time of his resignation from Moog, Pilkington held the position of Software Manager and worked at Moog's Torrance, California facility. Pilkington's last known home address is 1281 Cabrillo Avenue, Unit 401, Torrance, California 90501.

14. Defendant Misook Kim is a resident of the State of California. Kim was employed by Moog from on or about January 21, 2013 to December 18, 2021. At the time of her resignation from Moog, Kim held the position of Software Engineer and worked at Moog's Torrance, California facility. Kim's last known home address is 2120 Bridgeport Way, Torrance, CA 90503.

15. The true names and capacities, whether individual, corporate, associate, or otherwise, of defendants DOES 1 through 50, inclusive, are presently unknown to Plaintiff, who therefore sues said defendants by such fictitious names and will ask leave to amend the Complaint to show their true names and capacities when they

have been ascertained. Plaintiff is informed and believes and thereon alleges that each of the defendants designated herein as DOE is responsible in some manner for the events and happenings referred to in this Complaint.

16. At all relevant times, all Defendants were agents of and acting on behalf of each other.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331 because this action arises, in part, under the Defend Trade Secrets Act, 18 U.S.C. § 1836, *et seq*. ("DTSA"). The DTSA additionally states that "[t]he district courts of the United States shall have original jurisdiction of civil actions brought under this section." 18 U.S.C. § 1836(c). This Court has jurisdiction over Plaintiff's state law claims under 28 U.S.C. § 1332 because the parties are of diverse citizenship and the amount in controversy exceeds $75,000, exclusive of interest and costs.

18. This Court maintains supplemental jurisdiction over Moog's state and common law claims pursuant to 28 U.S.C. § 1367.

19. This Court has personal jurisdiction over Defendants because each of them resides in the state, and they have committed the torts alleged below within the state. The contracts at issue were performed at least partially in California. Further, this case was transferred to this jurisdiction and venue from the Western District of New York on or around December 15, 2022 pursuant to 28 U.S. Code § 1404.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because, as alleged below, a substantial part of the events giving rise to Moog's claims occurred in this district and/or the Defendants are subject to the Court's personal jurisdiction in this district with respect to this action. Further, this case was transferred to this jurisdiction and venue from the Western District of New York on or around December 15, 2022 pursuant to 28 U.S. Code § 1404.

MOOG'S STOLEN AND MISAPPROPRIATED TRADE SECRET FLIGHT CONTROL SOFTWARE AND OTHER DATA

21. Moog is a worldwide designer, manufacturer and integrator of precision control components and systems. The company offers a wide range of aircraft controls, space and defense controls, industrial systems and medical devices. Moog additionally has designing and manufacturing capabilities in motion control systems and components, control and power electronics, software, and fiber optics.

22. Moog designs, manufactures, and integrates precision motion and fluid controls and systems for various applications in the aircraft, aerospace, automated industrial machinery, marine, medical equipment, oil and gas, defense, power generation, construction, and simulation industries, and operates a network of manufacturing facilities in the United States, as well as in countries such as the United Kingdom, the Philippines, Germany, China, Italy, Brazil, India, the Czech Republic, Costa Rica, Luxembourg, Canada, the Netherlands, Lithuania, Ireland, and Japan.

23. Moog designs and manufactures the most advanced motion control products for aerospace, defense, industrial and medical applications – applications where precise control of velocity, force, acceleration and fluid flow are critical. Moog's motion control portfolio includes all forms of actuation technology, sophisticated control and power electronics and system software. Moog is a leading integrator of precision motion control systems.

24. The company's largest business segment is aircraft controls, which generates revenues from military and commercial aircraft in addition to aftermarket support.

25. As part of its motion control product portfolio, Moog develops software that governs flight controls for airplanes and other aircrafts, including helicopters. Moog has been in the business of development, testing, and certification of flight control software and applications since at least as early as

1999.

26. Among its many offerings, Moog develops software that "pairs up" with the hardware computers contained inside aircraft. Moog's flight control software provides utilities that the particular airplane application can use to interface with the hardware that the pilot is using in the aircraft. For example, when a pilot moves a control in the cockpit, Moog's software reads the control and moves the particular component of the airplane. Moog's flight control software also has actuation functions. In short, Moog's flight control software works in tandem with an aircraft's computer to control its flight and navigation functionality.

27. Modern flight control systems rely on a complex array of computers (hardware and software), wiring, component redundancy, power sources (electrical and/or hydraulic), control inceptors, and actuation to control the vehicle. Each one of these components plays a critical role in the operation of aircraft vehicle control. The sum of all these parts working simultaneously and in concert constitutes the flight control system of an aircraft.

28. Different types of technologies relating to flight actuation include the following:

- **Mechanically Signaled System:** With this technology, control inputs are wired directly to an actuator that may be electrically or hydraulically powered. The actuator can directly decode the electrical signals sent to it in order to move the actuator and, in turn, the vehicle surface that it is attached to.
- **Fly-by-Wire ("FBW") System:** With this technology, control inputs are wired to one or more computers, called a flight control computer or "FCC," that is used to monitor and control the flight control system through electronics and software. This computer can manage complex monitoring and decision-making to ensure the safety and control of the vehicle. The computer will send electrical commands to the actuator to

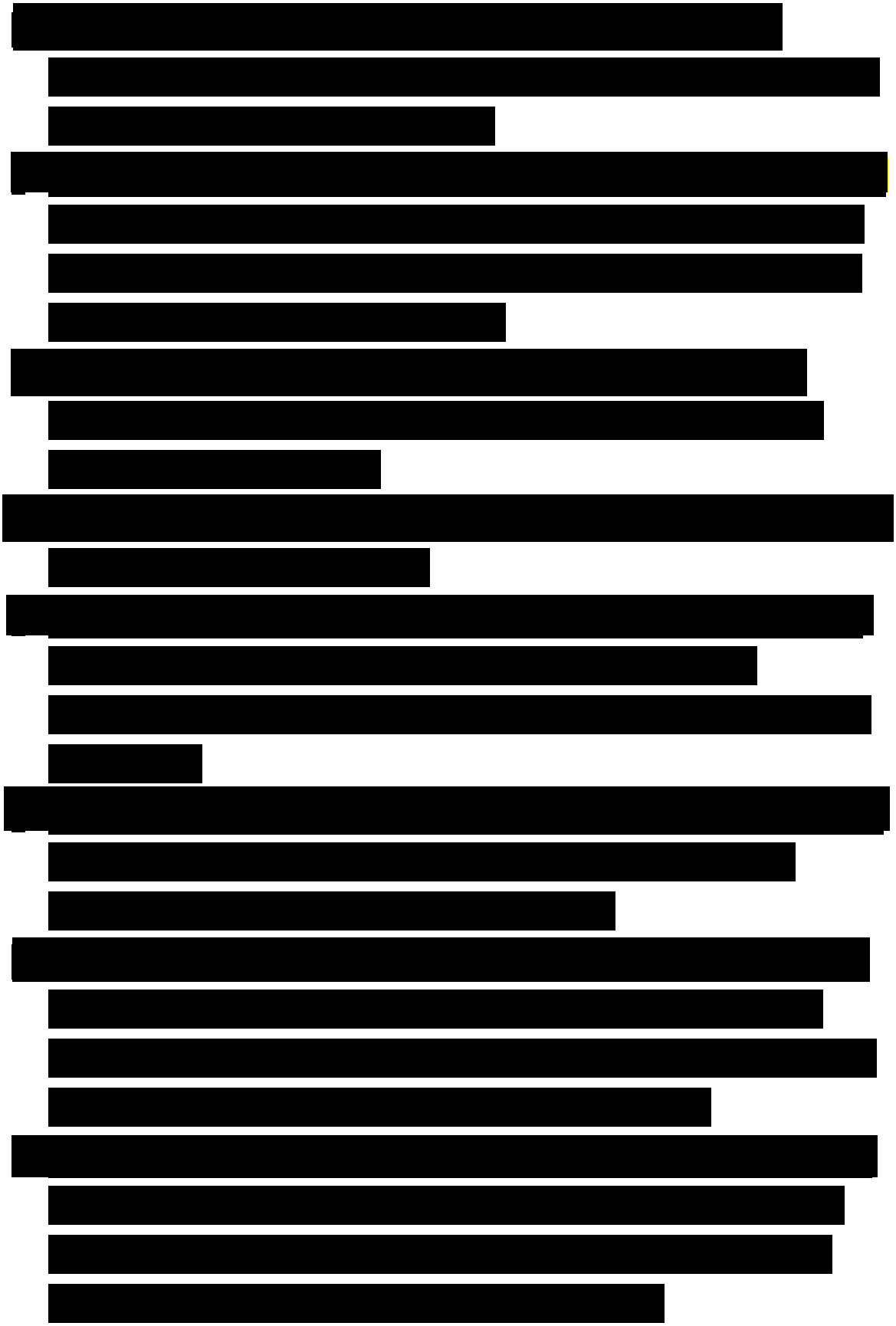
move the surfaces of the vehicle and receive feedback from the actuators on their performance.

- **Electrohydrostatic Systems ("EHA"):** These electrohydrostatic actuator systems, which can be part of a fly-by-wire actuator system, receive electrical signals from one or more FCCs and receive electrical power from one or more centralized power supplies which may be a battery, conditioned power from a generator, auxiliary power unit, or other source. These actuators then use the electrical power to drive a small, localized hydraulic pump to move the actuator. Differing levels of mechanical advantage, force, and speed are obtained by adjusting the stroke and diameter of the piston relative to the capabilities of the local pump.
- **Electromechanical Systems ("EMA"):** Like the electrohydrostatic actuators, electromechanical actuators receive electrical signaling from one or more FCCs and electrical power from one or more centralized electrical power sources as described above. The primary difference between the electromechanical system and the above systems is these actuators are fully electric and are controlled only by a motor or multiple motors controlling the movement of the actuator (as opposed to a hydraulic pump and valving system found in the electrohydrostatic actuator systems). Differing levels of mechanical advantage and actuator strokes are obtained by adjusting gear ratios and drive train designs (rather than hydraulic piston areas and pressures). Both electromechanical and electrohydrostatic actuators can be made to have extremely low probabilities of failure by employing a system of redundancy. To do this, typically three separate actuators will be arranged within one electromechanical actuator so that if any of the internal actuators fail, the remaining two can easily deliver the appropriate force and stroke required to maintain flight control.

29. Research, development, testing, and evaluation related to the implementation, deployment, manufacturing and certification of flight control systems is central to the trade secret technologies at issue in this case. The following attributes provide an overview of the trade secrets and other proprietary data which have been stolen and misappropriated by Defendants.

[redacted]

[1] The term "process" as used in this Amended Complaint generally refers to a defined set of steps required to be followed for the design and development of hardware and/or software for safety-critical aerospace applications.



[redacted]

30. With this general overview, Moog now identifies the various types of trade secrets and proprietary data stolen and misappropriated by Defendants in this case.

Toolset #1 - Software Engineering Process:

31. A "toolset" as used herein is a process or component used to aid in the

development of an item for a program. One example would be the operating system software used in the electronics for the Boeing 787 program as it is a subset of the whole software. Another example would be the process by which source code is developed by engineers to satisfy government aerospace standards.

[redacted]

33. [redacted]

[redacted]

Toolset #2 - Platform

[redacted]

[redacted]

Toolset #3 – eRTOS

[redacted]

[redacted]

Toolset #4 - AMP

[redacted]

Toolset #5 – Neo[2]

42. [redacted]

[redacted]

[2] Toolsets Nos. 1 through 5 above are collectively referred to as the "Toolsets."

Trade Secret Commercial and Military Programs

43. The data that has been misappropriated by Defendants relates to at least 21 programs, corresponding to 12 military programs and 9 commercial programs, as identified in the below tables[3]:

Military Programs (12)	
Northrop Grumman	B-2
	X47B
	TERN
Boeing	F15SE
	UCLASS
Lockheed Martin	F35
Bell	V280
Moog internal aliases for sensitive government programs	EHFCAS
	Emerald
	Sensitive Government Program 2
	Sensitive Government Program 1
	Bullfrog (predecessor to Sensitive Government Program 2)

Commercial Programs (9)[4]	
Boeing	747-8
	787
Airbus	A350
COMAC	C919
Embraer	E2

[3] To be clear, the files stolen in this case go beyond the Programs and Toolsets identified in the tables.

[4] Gulfstream G650, G700, and G800 are different programs and aircrafts but have similar high-lift systems and so Moog will sometimes group them together.

Gulfstream	G280
	G650
	G700
	G800

44. The trade secrets at issue for each of the military and commercial programs listed above include the following subcategories:

- **747:** [redacted]
- **V-280:** [redacted]
- **B-2:** [redacted]
- **TERN:** [redacted]
- **X-47B:** [redacted]

- **747-8:** [redacted]
- **A350:** [redacted]
- **G280:** [redacted]
- **G650, G700, and G800:** [redacted]
- **F15SE:** [redacted]
- **F35:** [redacted]
- **UCLASS:** [redacted]
- **C919:** [redacted]
- **E2:** [redacted]
- **Sensitive Government Program 1:** [redacted]
- **Bullfrog:** [redacted]

- **Sensitive Government Program 2:** [redacted]
- **Electro-Hydraulic Flight Control Actuation System ("EHFCAS"):** [redacted]
- **Emerald:**[5] [redacted]

Other Trade Secrets at Issue

45. Defendants misappropriated additional trade secrets that do not necessarily fall under the Toolsets or Programs described above. Some of these trade secrets (described below) are not necessarily technical in nature, but are in the nature of business trade secrets.

- **Cost Estimating Templates:** [redacted]

[5] The 21 Moog programs described herein are collectively referred to as the "Programs."

[redacted]

- **Autopilot Program:** [redacted]

- **Proposal Data:** [redacted]

- **Reid Raithel:** [redacted]

[redacted]

46. The materials identified above in Paragraphs 31 through 45 will be collectively referred to herein as the "Stolen Trade Secrets." The Stolen Trade Secrets are reflected in approximately 291,000 unique files stolen by Defendants, not inclusive of duplicates or different versions of the same files. Approximately a million of the files stolen by Defendants constitute duplicates or different versions of the same files for which Moog seeks trade secret protection over, and these duplicates or different versions contain overlapping information with the approximately 291,000 unique files which reflect the Stolen Trade Secrets.

Economic Value of the Stolen Trade Secrets

47. The Stolen Trade Secrets have very significant economic value to Moog. For example, a Toolset like Platform allows Moog to tailor its aircraft-specific software very quickly based on the particular needs of that aircraft or project. Platform provides the base flight control software such that Moog only needs to develop an additional layer of software for the flight controls of a particular type of aircraft.

48. The Stolen Trade Secrets contain Moog's most valuable, sensitive, and proprietary information.

49. The novel realization of an adaptable flight control software (such as Platform) provides Moog a considerable and valuable competitive advantage in the marketplace. The uniquely-adaptable software such as Platform allows Moog to be uniquely competitive and the front-runner in obtaining contract awards from commercial or military customers.

50. The Stolen Trade Secrets took over 16 years, and many millions of dollars, to develop. For example, building each iteration of the Platform software required 10 full-time software engineers over a period of two to three years. Some of the Toolsets and Programs took over 100,000 engineering hours to develop, test,

and certify.

51. Moreover, the testing and certification requirements for flight control software are extremely vigorous and costly. Before any flight control software is approved by the Federal Aviation Administration ("FAA") or similar governing bodies around the world, it must be vigorously tested and certified. Different types of testing and analyses are required. It takes twice as long to test and certify flight software than it does to construct it. Testing and certification generally constitutes two-thirds of Moog's total cost to build flight software.

52. Moog has also invested many millions of dollars in building, testing, and certifying the aircraft project-specific software applications that sit on top of Toolsets like Platform.

53. Were a competitor to obtain and be allowed to exploit the Stolen Trade Secrets, it would provide a huge competitive advantage to that company. If a third party had possession of the Toolsets, including the code, testing, and certification requirements, the third-party company could easily "click and build" a project specific software on top of the base software in a short amount of time and potentially saving hundreds of thousands of engineering hours. The only thing the party would need to build a project-specific application is an electronic computer from a particular aircraft to connect to.

Stolen Non-Trade Secret Data

54. In addition to the Stolen Trade Secrets reflected in approximately 300,000 files (as well as approximately a million duplicate or alternative versions of the same files), Defendants also stole from Moog approximately 107,000 files which Moog does not seek trade secret protection over in this case. Files from each of the Programs discussed above are included in this group of non-trade secret data. The stolen non-trade secret files include sensitive files which are owned by Moog, have value to Moog, but do not rise to the level of trade secrets. This bucket of stolen non-trade secret files includes, but is not limited to:

- Subversion Logs: Moog's software version control tool is subversion, which keeps track of changes made to source code and other files. These files are owned by Moog and are not disclosed to third parties or the public.
- Intermediate Build Files: Moog uses tools to create an executable from the source code files. In the process of making this executable, intermediate files are made. These intermediate files are created from the source code and are a temporary product in the steps to make an executable. Some of these are used by the tool when a developer is debugging the source code. These files are owned by Moog and are not disclosed to third parties or the public.
- Test Equipment Files: Testing environments have commercial tools intermixed with code created by Moog to create the final test environment. In creating the final test environment, there are intermediate files created in the process. These files are owned by Moog and are not disclosed to third parties or the public.
- Results and Log Files from Verification Runs: Moog formally tests its software flight code. During these test execution runs, steps of the testing and outcomes of the testing are logged in log files detailing how the test ran. These files are owned by Moog and are not disclosed to third parties or the public.
- Custom Code for Software Utilities: Moog uses commercial tools to load its software. Custom code is generally added on top of this commercial code, to make an automated method to upload and download data from the processor. This custom code added to these files is owned by Moog and not disclosed to third parties or the public.
- Customer Data: Pursuant to contracts with various third parties, Moog maintains possession of customer documents and data. Moog holds these

documents in trust on behalf of third-party customers, including companies such as Northrop Grumman.

- Model Intermediate Files: Moog makes Simulink models to simulate either Moog hardware or third-party customers' hardware. These models create extra files when they are executed. These files are owned by Moog and are not disclosed to third parties or the public.
- Developer Environment Files: Moog uses different developer environments to create its software source code. These developer environments save settings for the programmers to customize the environment for them. These files are owned by Moog and are not disclosed to third parties or the public.
- Instrumented Files for Code Coverage: Moog uses tools to determine if the software code is covered by testing. The tool uses modified versions of the source code files to track whether a test is testing each line. These modified source code files are owned by Moog and are not disclosed to third parties or the public.
- Electronic Schematics Intermediate Files: Moog creates electronic schematic files to design its electronics. As this is created and tested, extra files are created by the tools in which these schematic files are created. These extra files are owned by Moog and are not disclosed to third parties or the public.
- Doxygen Intermediate Files: Moog uses a commercial tool to comment on and explain its source code. It is also used to create design documents from text embedded within the code. This tool saves off versions of the source code with its embedded text. These source code version files are owned by Moog and are not disclosed to third parties or the public.
- Project Status Documents: Moog maintains documents which track the progress of activities on certain flight control programs. These documents

include metrics on program development and other status reports. These files are owned by Moog and are sometimes disclosed to third parties in limited circumstances.

55. As described further below, former Moog employee and subsequent Skyryse employee Reid Raithel stole approximately 27,000 files on his way out the door from Moog before joining Skyryse. Approximately 13,000 of these files reflect Moog's trade secrets. The remaining approximately 14,000 files represent stolen non-trade secret data which include sensitive files owned by Moog, have value to Moog, but do not rise to the level of trade secrets. This bucket of stolen non-trade secret files includes, but is not limited to:

- Moog Test Capability and Equipment Supplier Information Documents: Moog maintains documents which reflect results and capability of its test lab capabilities as well as lists of suppliers capable of making test equipment or other types of products for the Moog labs, and information about suppliers' abilities to make test equipment for Moog labs. These files are owned by Moog and are sometimes disclosed to third parties in limited circumstances.
- Management Meeting Documents: Moog maintains documents related to management and department meetings, including notes, company news, and departmental strategies. These files are owned by Moog and are not disclosed to third parties or the public.
- Recruiting Documents: Moog maintains documents related to recruiting efforts, including interview notes, compilations of resumes of select candidates, and resumes of certain Moog employees. This collection of files is owned by Moog and is not disclosed to third parties or the public.
- Organizational Documents: Moog maintains documents reflecting organizational charts in various departments, including documents to show Test Equipment staffing by discipline, experience, and capability level.

These files are owned by Moog and are sometimes disclosed to third parties in limited circumstances.

- Management Files: Moog maintains documents related to facilities, employees, and workflow reflecting training, operations, issues found, and management plans. These files are owned by Moog and are not disclosed to third parties or the public.
- Program Files: Moog maintains program-related files which contain information related to flight control programs or contain images of hardware related to programs. These files are owned by Moog and are sometimes disclosed to third parties in limited circumstances.

56. The materials identified above in Paragraphs 54 through 55 will be collectively referred to herein as the "Stolen Non-Trade Secret Data."

MOOG'S MEASURES TO PROTECT ITS INTELLECTUAL PROPERTY

57. Given the confidential and valuable nature of the Stolen Trade Secrets, as well as the Stolen Non-Trade Secret Data, Moog takes the security of its software and documentation very seriously, and employs several important security measures to control and limit access to the software and protect against theft or misuse thereof.

58. Moog employees are required to sign confidentiality and/or non-disclosure agreements. Moog employees are also required to sign Moog internal proprietary information agreements, as well as third party proprietary information agreements when working on certain project-specific applications, including sensitive government projects. Moog employees are required to sign patent assignment agreements.

59. Moog also requires its departing employees to sign an exit form wherein each individual confirms they have been provided access to Moog's proprietary and trade secret information, have returned all Moog IP upon departure, and have not maintained access to or copies of any digital record of belonging to

Moog.

60. Further, the Stolen Trade Secrets and Stolen Non-Trade Secret Data are housed on a secure server at Moog. Moreover, only certain employees at Moog have access to materials within the software database. Access to materials within the software database is authorized on a "need to know" basis that must be approved by the lead on the relevant software program. For example, an employee can work on a software program but not be given access to the software database if the program lead determines that the employee does not require access to the software database. Even within the secure software database, there is additional limitation and segregated access to certain program materials within the secure environment. Each program has a separate branch and location on Moog's secure servers and databases. In order to have access to the Toolsets and Programs, a Moog employee would need five separate credentials.

61. Moreover, the Toolsets and Programs as applied to military projects are extremely sensitive to the US Government. Only a limited number of individuals have the necessary access credentials to work on the Sensitive Government Programs. To obtain such access credentials is time consuming and requires extensive vetting and clearances.

62. Under its government contracts, Moog is obliged to implement extensive security measures to safeguard and protect sensitive information. These security measures include, *inter alia*, access restrictions, authentication, encryption, physical protections, and specific training for employees. Moog also adheres to additional requirements and protections for sensitive data for certain of its government customers.

63. Further, Toolsets such as Platform are designed to prevent hacking or reverse engineering. It cannot be reverse engineered from an aircraft computer that has used the software.

64. With respect to its facilities, Moog has controlled access into its

buildings, and all employees must undergo security screening and a background check before being hired.

65. Every new Moog hire (including any software engineer) is required to review the then-current Moog employee handbook and acknowledge the requirements therein in writing, either through a signed paper form or an electronic acknowledgment. Pilkington acknowledged receipt and agreed to abide by Moog's employee handbook in writing on July 30, 2012. Kim acknowledged receipt and agreed to abide by Moog's employee handbook in writing on January 21, 2013. A true and correct copy of the acknowledgments signed by Pilkington and Kim are attached hereto as **Exhibit A**. A true and correct copy of the Moog employee handbook in effect when these acknowledgments were signed (the "Employee Handbook") is attached hereto as **Exhibit B**. The Employee Handbook provides that Moog employees will receive access to confidential and proprietary information, and that disclosure to any outside party is prohibited, including after employment has been terminated. It also emphasizes that Moog employees may not retain any copies of Moog's confidential and proprietary information.

66. Moog also has a robust written policy governing its intellectual property, including its internal proprietary, confidential, and trade secret information. This written policy is made available to every Moog employee, including all software engineers. This written policy, among other things, defines Moog's proprietary and trade secret information, provides strict protocols for storing, designating, and transmitting such information, and prevents any third-party disclosure of such information. Moog requires its employees (including all software engineers) to attend a training on Moog's proprietary and trade secret information, which summarizes the contents of Moog's written IP policy. Pilkington completed Moog's trade secrets training in July 2012 and again in October 2016, and Kim completed the training in February 2013 and again in January 2015. Kim and Pilkington were bound by the Moog IP policy and trade secrets training. Moog

employees are also required to complete annual ethics training.

67. Moog employees are required to return any trade secret information accessed or possessed while in their employment at Moog. Moog exit paperwork for employees includes an acknowledgement of continuing obligation to protect confidentiality upon termination.

68. Moog has implemented cybersecurity measures in accordance with NIST Special Publication 800-171, consistent with current Department of Defense requirements.

69. Moog has a written policy that is made available to software engineers and other Moog employees regarding its intellectual property and confidential, proprietary, and trade secret information. Among other things, this written policy defines Moog's proprietary and trade secret information and includes strict protocols regarding the storage, designation, and transmission of such information. Moreover, this written policy prohibits third-party disclosure of such information.

70. Moog's Jira and Subversion repositories store the flight control software, source code, software artifacts, and related documents for each of Moog's flight control programs at issue in this case. The lead on the software program approves access to these software databases, and such access is on a "need to know" basis. For example, an employee can work on a software program but not be given access to the software database if the program lead determines that the employee does not require access to the software database. A specific request and approval for access to Jira and Subversion repositories is needed in order to get access to those repositories. The timing of any user's access to the software database, and revocation of access, is tracked by Moog using software tools. For example, Moog uses Ivanti Device Control, which is an endpoint policy enforcement solution. This software provides endpoint encryption allowing the administrator to enforce certain security policies on removable devices. The program allows the user to see which files have been downloaded or copied from Moog's internal servers onto removable

devices (e.g., external hard drives, USB devices, etc.).

71. Moog access control policies limit system access to authorized users and functions based on employee roles and responsibilities.

72. As to third-party contracts with suppliers and/or customers that include delivery of Moog trade secret materials, Moog requires confidentiality agreements and/or non-disclosure agreements that govern the provision of such information and have strict requirements regarding the purpose and scope of disclosure as well as return and/or destruction.

73. Every Moog flight software source code file contains restrictive language such as: "*MOOG PROPRIETARY and CONFIDENTIAL INFORMATION; This technical Data/Drawing/Document contains information that is proprietary to, and is the express property of Moog Inc., or Moog Inc. subsidiaries except as expressly granted by contract or by operation of law and is restricted to use by only Moog employees and other persons authorized in writing by Moog or as expressly granted by contract or by operation of law. No portion of this Data/Drawing/Document shall be reproduced or disclosed or copied or furnished in whole or in part to others or used by others for any purpose whatsoever except as specifically authorized in writing by Moog Inc. or Moog Inc. subsidiary.*"

74. The Stolen Trade Secrets also generally contain restrictive language such as: "MOOG PROPRIETARY AND CONFIDENTIAL INFORMATION."

CENTRAL MOOG TEAM WORKING ON THE STOLEN TRADE SECRETS

75. Gonzalo Rey (former Director of Engineering and Chief Technology Officer) and Sathyanarayana Achar (former Engineering Technical Fellow) were the first two Moog employees to sponsor and oversee the development of Moog's Toolsets (including the Platform base software) beginning in 2007. They have the most institutional and technical knowledge regarding the Toolsets, as well as its relationship with project-specific applications which sit on top of the Toolsets. They

are now employed by Skyryse.

76. Michael Hunter and Todd Schmidt are two senior level engineers who have worked on and managed the programs that created certain of the Toolsets (including Platform), and the related commercial Programs, since 2007. Both were solicited for employment by Skyryse.

77. Defendant Robert Alin Pilkington (former Senior Staff Engineer) was the lead architect (software engineer) on eRTOS. eRTOS is the second iteration of the Platform base software used for military purposes. At Moog, Pilkington and his team built eRTOS beginning in 2013. As of 2016, Pilkington reported directly to Hunter. In November 2021 and at the time of his departure from Moog, Pilkington and his team were working on military project Sensitive Government Program 2, which sits on top of the eRTOS base software. They all had heightened access credentials to work on this project.

78. One of the individuals working under Pilkington was Defendant Misook Kim, a Senior Staff Engineer. Kim had worked under Pilkington's supervision for several years. Pilkington joined Moog in 2012 and brought Kim with him. While at Moog, Kim was extremely loyal and obedient to Pilkington and routinely demonstrated that she was willing to perform any task that Pilkington needed or asked of her.

79. Eric Chung joined Moog in 2013, Lawrence Chow joined Moog in 2014, and Mario Brenes joined Moog in 2018, and all three worked on Pilkington's team and under his supervision. All the individuals listed in this paragraph ultimately left Moog for Skyryse.

80. As of the Fall of 2021, Moog had twenty-nine (29) software developers/engineers in the Buffalo, New York area and twenty-two (22) in the Los Angeles, California area working on Moog's Toolsets and Programs.

MOOG'S DEVELOPMENT OF AUTOMATED FLIGHT TECHNOLOGIES BEGINNING IN 2012

81. Moog began to pursue and develop automated flight technologies beginning in 2012. The initial endeavor was in connection with automated flight projects for the Robinson R-44 helicopter. Between 2012 and 2014, Moog pursued a [redacted]

82. [redacted]

AS SKYRYSE MAKES PROMISE AFTER PROMISE TO INVESTORS, IT GOES TO MOOG TO TRY AND SATISFY THOSE PROMISES

83. Moog has an Aircraft Group and an Innovation and Technology Group, which has its own subgroup for Growth and Innovation dating back to early 2018. The purpose of the Growth and Innovation Group is to explore new and innovative business opportunities for Moog outside of its existing business channels. The focus of the Growth and Innovation Group evolved over time, but gradually became more centered on flight controls and the front end of aircraft functionality. However, the group also was increasingly focusing on helicopter flight control when they first

encountered Skyryse.

84. In 2018, Moog's Growth and Innovation Group began exploring a potential business opportunity with Defendant Skyryse, which at that point was a very new company, having just been formed in 2016 by Mark Groden.

85. Mr. Groden was 26 years old at the time of the company's founding. He was described in the press as a "wunderkind[]…who at age 15 built an unmanned fixed-wing VTOL that was used by the U.S. military." His Forbes profile states that when he "was 16, he joined the U.S. Air Force lab at Case Western, where he built an unmanned aerial vehicle."

86. On August 30, 2018, Moog employee Jeff Ehret reached out to Skyryse's general e-mail address about a potential discussion. In the e-mail, Ehret stated: "Moog has previously demonstrated an optionally piloted Robinson R44 flight capability in 2014 . . .We are currently working on a solution that offers the ability for full autonomous flight including take-off and landing." Skyryse CEO Mark Groden expressed interest and noted in response: "[redacted] ultimately and Moog is the only company who can build one." Moog and Skyryse then engaged in a series of discussions and meetings, in which Skyryse explained its business plan.

87. Based on Skyryse's explanations about its business plan, Moog believed there was real potential for opportunity based on Moog's then-existing capabilities and desire to enter into new markets. During these initial discussions in late 2018, Skyryse represented that it wanted to offer on-demand helicopter transportation to the general public as a "commuter service" (an "Uber-of-the-skies" type of business), through the use of automated flight system technology. Under this potential structure, Moog would provide the helicopter flight control systems (including flight control software, actuators, and computers), and Skyryse would install and implement this technology into its business. Skyryse would have its own central computers which would send a command to Moog about where a certain

helicopter would fly to, and Moog would take care of the flight control aspect (including takeoff, navigation, and landing).

88. Skyryse further indicated that it wanted to own the Supplemental Type Certification ("STC") for the unmanned, automated flight system for the R-44 helicopters.

89. Any type of software, hardware, or other technology that goes into a helicopter requires a STC issued by the FAA. This means that the FAA has authorized the certain technology or software to go into the helicopter. Because Skyryse wanted to own the STC for this technology, Moog demanded (and Skyryse agreed) that Skyryse would perform and take responsibility for all installation of Moog's technology into Skyryse's R-44 helicopters.

90. Under Skyryse's initial proposed business model, Skyryse's goal was to eventually offer unmanned helicopters through an automated flight system provided by Moog. However, in the early stages of its business Skyryse intended to have a safety pilot on board that could override the automated flight system and take control if needed.

91. As these business discussions progressed and to facilitate an exchange of information to evaluate a potential business opportunity, on October 24, 2018, Moog and Skyryse entered into a "Proprietary Information and Nondisclosure Agreement" (the "2018 NDA"), a true and correct copy of which is attached hereto as **Exhibit C**. The 2018 NDA's express scope was for the "[e]xchange of business and technical information in various forms and forums."

92. At the time of the initial NDA, Skyryse had closed $25 million in seed and Series A funding – on or around August 28, 2018. In press articles in connection with the funding, Skyryse was described as having "aspirations to work on technology for FAA-approved vertical take-off and landing (VTOL) aircraft."

93. On March 11, 2019, Groden shared a Skyryse pitch deck with various Moog personnel, a true and correct copy of which is attached as **Exhibit D**.

Skyryse's stated mission was to "Free the world from travel time." The pitch deck provided various statistics and metrics about travel times in the Los Angeles market, and potential revenue options by providing a commuter flight service "that directly replaces UberBlack." Skyryse described its business as a "commuter service." Nowhere in the pitch deck did Skyryse mention anything about developing its own autonomous flight systems or flight control software.

94. As discussions continued to progress, on March 15, 2019, Moog and Skyryse entered into another "Proprietary Information and Nondisclosure Agreement" (the "2019 NDA"), a true and correct copy of which is attached hereto as **Exhibit E**. The 2019 NDA contains the same material terms as the 2018 NDA. However, the 2019 NDA's express scope was for: "Discussion of integration of Moog's flight control systems /subsystems / components and associated autonomous control technologies with Skyryse's aircraft platforms and associated autonomous control technologies."

95. Under these NDAs, the Parties agreed not to disclose any proprietary information disclosed by the other parties, and the receiving party of such information could only use it for the limited purpose of the contemplated engagement between Moog and Skyryse. (*Id*. at § 2). The NDAs both had an effective term of 10 years. (*Id*. at § 5). The Parties agreed that any breach of the NDAs would result in "irreparable and continuing damage" and that the "non-breaching Party shall be entitled to seek injunctive relief, without the necessity of posting a bond." (*Id*. at § 8). Both the 2018 NDA and 2019 NDA also contained New York choice of law provisions.

96. Moog and Skyryse's business relationship was contemplated to be conducted in four separate phases, with the Parties agreeing to enter into a separate contract before each phase. On May 31, 2019, Moog and Skyryse entered into a "Statement of Work for Phase 1 of Safe Autonomous Flight Evolution (SAFe) of the Robinson R44" (hereafter, the "SOW1"), a true and correct copy of which is

attached hereto as **Exhibit F**.

97. Section 2 of the SOW1 describes the background of Moog and Skyryse. Skyryse is described as being [redacted] Moog is described as being "[redacted]

98. Section 3 of the SOW1 describes the responsibilities of each party. Skyryse's stated responsibility was solely to serve [redacted] Skyryse's specific duties included: [redacted]

99. Section 4 of the SOW1 describes the program overview: [redacted] Thus, the Parties expressly agreed that their obligations would be limited to SOW1 and any additional SOWs would have to be mutually agreed by the parties.

100. Section 4.1 states: [redacted] Section 4.1.1 also clarifies: [redacted]

101. Section 4.1.2 describes the various tasks to be completed by both parties under Phase 1:

[redacted]

102. In terms of pricing, Skyryse agreed to pay Moog [redacted] for phase one for one unit of development hardware and [redacted]

103. Similar to Section 4, Section 5 provides again: "[redacted]." Thus, the Parties again expressly agreed that their obligations would be limited to SOW1 and any additional SOWs would have to be subsequently mutually agreed-to by the parties.

104. In Section 7.2 (Moog Value Addition), Skyryse acknowledged that "[redacted] Skyryse further acknowledged that [redacted]

105. Section 9 (Appendix) further made clear that [redacted] ” (emphasis added.) In other words, neither party was required to proceed with an SOW for Phase 2.

106. On June 3, 2019, Moog and Skyryse entered into a “Terms and Conditions of Sale” (the “T&C”), a true and correct copy of which is attached hereto as **Exhibit G**. The T&C contains provisions that the Parties cannot use each other’s pre-existing proprietary IP for any other purpose than performing under the T&C, and expressly prohibited reverse engineering. (*Id*. at §§ 20, 23).

107. Section 23 of the T&C incorporates by reference the 2019 NDA. Under Section 39, the Parties agreed they could amend the T&C as mutually agreed to in writing.

108. Section 32 of the T&C describes termination. Section 32.1 provides that “termination must be transmitted as a written notification” and must “specifically identify the work being terminated.” Section 32.2 provides that “[p]romptly after the effective date of the termination, [Moog] shall submit its invoice, and be paid the Agreement price, for articles completed but not yet invoiced.” It further provides that Moog shall “submit a termination claim for an Equitable Adjustment as may be appropriate as the result of the termination, considering partially completed work, termination costs, and other facts.”

109. Before the parties were to explore Phase 2, Skyryse intended to take its system live to the public. On information and belief, Skyryse’s launch did not go as planned and was not successful.

110. Indeed, in connection with its contemplated Series B financing round, Skyryse reached out to Moog for a potential investment. Specifically, on September 14, 2019, Gonzalo Rey reached out to Moog’s CEO John Scannell to gauge Moog’s interest in investing upwards of $5 million into Skyryse. On September 20, 2019,

Scannell declined Rey's proposal for investment, and noted that Moog looked forward to continuing its work with Skyryse pursuant to SOW1 and the underlying agreements.

111. By October of 2019, Skyryse stopped its business operations, fired many of its employees, and was looking to pivot its business model.

112. On December 17, 2019, Skyryse issued a press release proclaiming that it was offering an autonomous flight system as part of a flight control operating system. It called the automation technology "Flight Stack." On the same date, it revealed that it had obtained another $13 million in financing.

113. Skyryse additionally revealed "Luna," which was very similar to Moog's name for its autonomous flight system previously discussed with Skyryse, "Lucy." "Luna" was described at the time as "a Robinson R44 helicopter retrofitted with the company's autonomy technology."

114. Skyryse had pivoted into exactly what Moog was doing, and the previously separated and defined roles for Moog and Skyryse became blurred.

115. On February 12, 2020, certain Moog and Skyryse personnel held an in-person meeting at Moog to review the actuation and pedal sense system design (Critical Design Review) under the existing SOW1. At the conclusion of that meeting, in a smaller group meeting with Gonzalo Rey of Skyryse and Dave Norman of Moog, Rey advised Moog that Skyryse wanted to make changes to their system and there was a desire to stop the current work under SOW1, cancel the underlying purchase order, and shift the nature and scope of the parties' engagement to a new, expanded effort. Specifically, Rey conveyed that Skyryse wanted to focus more on [redacted]. This was a far departure from SOW1, which focused on a [redacted].

116. Moog determined that Skyryse's requested changes and expanded scope of work was a vast departure from the projects described in SOW1, and

therefore SOW1 would need to be drastically revised or cancelled and a revised or new statement of work would need to be discussed with Skyryse.

117. On February 28, 2020, Moog sent Skyryse a draft statement of work for a proposed SOW2. The scope of the draft SOW2 "[redacted]." Also, unlike SOW1, the draft SOW2 stated that "[redacted]."

118. Later that same day, on February 28, 2020, Rey provided his input and comments to the draft SOW2 and conveyed his desire to get the draft SOW2 completed as soon as possible. On March 6, 2020, Moog sent Skyryse a revised draft SOW2 in an effort to try to move forward with Skyryse's requested change in the nature and scope of work.

119. Due to Skyryse's prior verbal requests to cancel the open purchase order underlying SOW1, on March 6, 2020, Moog Program Administrator Alan Kresse reached out to Skyryse, advising that pursuant to Section 32 of the T&C, Skyryse must provide formal written notification of termination of SOW1 and underlying purchase order. Kresse also sent a formal letter to Mark Groden of Skyryse memorializing his requests.

120. In response, on March 6, 2020, Gonzalo Rey from Skyryse indicated that he was jointly exploring with Moog "the possibility of finding a better win-win for Moog and Skyryse." Dave Norman from Moog responded a few days later, noting that the letter from Kresse was just "one means to come to an agreement on closing out the original SOW" but that Moog was "open to alternatives including PO revisions." and that it was in the Parties' "mutual interest to formalize our path forward." Norman also emphasized to Rey that Moog had "put in a significant effort to this point" and it would need to get paid for its work "before agreeing to Phase 2 SOW." There is nothing in this e-mail exchange suggesting Moog forced Skyryse to

cancel SOW1 with assurances the Parties would enter into additional SOWs.

121. On March 10, 2020, Gonzalo Rey of Skyryse and Tim Abbott, Dave Norman, and Paul Stoelting of Moog had a telephone call to discuss how to move forward with a revision to SOW1 to support transitioning to the proposed scope of work under the draft SOW2.

122. On March 16, 2020, at Skyryse's request, Moog sent Skyryse a draft revised SOW1 to remove work that would no longer be performed, and to reduce SOW1's scope to only reflect the work already performed by Moog under SOW1. This action would allow a clean transition from the no longer applicable designs of SOW1 to the new SOW2 scope under the existing purchase order.

123. On March 18, 2020, Gonzalo Rey of Skyryse asked Dave Norman of Moog for a rough order of magnitude estimates for existing charges and work already performed under the existing SOW1, and estimates for the new, expanded scope of work the parties were discussing.

124. On March 19, 2020, Tim Abbott from Moog e-mailed Rey from Skyryse, explaining that Moog had completed 30.8% of the work from SOW1 and thus was owed ~$970,000 from Skyryse. Abbott also provided an estimate for a revised purchase order based on a the new, expanded scope of work that was included in the draft SOW2 dated March 6, 2020 that Moog had sent Skyryse, totaling $4.22 Million for the revised purchase order value (the combined total of work performed on SOW1 and the work proposed under draft SOW2). In response, Rey expressly acknowledged: "***I understand how you get to the $970k***." (Emphasis added.)

125. Abbott clarified in a March 23, 2020 e-mail that the $3 million estimate in connection with the new, expanded scope of work was only for "the experimental R66 flight test only in accordance with the revised statement of work that we have sent for SkyRyse review." Abbott sent another e-mail on March 25, 2020 breaking down the $970,235.37 owed from Skyryse. Abbott further advised Rey that, because

of Rey's previously indicated preference to revise SOW1 and pay Moog for work completed under the existing SOW1, in order to facilitate the invoicing process pursuant to the T&C, Moog needed Skyryse to provide a letter "formally stating the intention to revise the current statement of work and allowing us to invoice you for work complete[d] to date." In response, Rey stated: "***I agree with the next step you describe***," and the revision letter would be sent "this week." (Emphasis added.) The purpose of this e-mail exchange is clear on its face—Moog needed Skyryse to formally confirm that it was revising SOW1 in writing as required by Section 32 of the T&C, and that Skyryse would pay Moog for work completed to date and thus Moog would not be on the hook for all deliverables under SOW1.

126. On March 31, 2020, Rey sent Moog a letter formally cancelling the purchase order for SOW1, a true and correct copy of which is attached hereto as **Exhibit H**. This was surprising to Moog given the ongoing conversations and stated preference by Skyryse to revise and modify SOW1 and the underlying purchase order, rather than cancelling it. Thus, it was Skyryse's decision to cancel SOW1 rather than to agree to modify it based on the parties' ongoing discussions and the revised SOW1 sent to Skyryse on March 16, 2020. On April 3, 2020, in response to Skyryse's cancellation of SOW1 and the underlying purchase order, Moog sent Skyryse a final invoice for $1,024,277.46 ($970,235.37 plus tax). Skyryse paid that amount and Moog closed out the invoice.

127. While all of these discussions were going on, on March 17, 2020, Skyryse next announced the launch of what it called "FlightOS." Skyryse's press release described FlightOS as "combining on-board computers and fail-operational flight control automation hardware to power a new class of envelope protection and emergency management. The system constantly monitors the aircraft's movement, stability, and flight path to ensure flight operations remain within all aspects of the flight envelope capabilities." It also proclaimed that with FlightOS, "on-board computers control all aspects of the flight envelope, manage the airframe's structural

and aerodynamic operating limits, and leverage exterior radar and sensors for real-time situational awareness." Skyryse also took a dig at Moog, proclaiming "[f]or decades, there has been little technological advancement in general aviation."

128. Notwithstanding these proclamations, on May 22, 2020, Skyryse issued a request for quote ("RFQ") to Moog, a true and correct copy of which is attached hereto as **Exhibit I**. The RFQ was sent by Tim Baptist of Skyryse, who was formerly Aircraft Group Vice President at Moog before leaving in February 2020. The Skyryse RFQ disclosed to Moog for the first time that Skyryse was seeking certification of its own FlightOS flight control software.

129. In the RFQ, Skyryse stated that it was "ramping up the second phase of the go-to-market program with the certification FlightOS on a light helicopter." The RFQ also states that Skyryse's "goal is to certify a system with a simplified pilot interface that makes flying safe and easy to learn for a broad cross-section of the public."

130. Skyryse was "seeking a teaming agreement with Moog" and sought a quote for up to "150 shipsets of production" based on Skyryse's proposed SOW and provided six general line items of what Skyryse was seeking from Moog, including development and delivery of a "single triple redundant actuator version," "side stick," "lab system," "flight test system," and "[c]ertification baseline system."

131. The RFQ based on Skyryse's own proposal for up to 150 shipsets is completely different than Moog's $4.22 Million estimate for "the experimental R66 flight test only" based on Moog's separate proposed SOW. The RFQ made clear that Skyryse was not interested in delivery of original equipment or the continuation of SOW1.

132. In short, Skyryse requested that Moog provide flight control computers and actuator systems for Skyryse to use and to implement Skyryse's flight control operating system software. Providing flight control computers and actuator systems for aircrafts was already an established line of business for Moog. So, Moog,

focused on innovative and new business opportunities, was reluctant to pursue that line of business with Skyryse, especially since Skyryse had changed its entire business plan and model compared to when Moog first started doing business with Skyryse.

133. Nonetheless, given the prior business relationship with Skyryse, and the fact that several former respected Moog employees worked at Skyryse, on June 17, 2020, Moog submitted a bid in response to Skyryse's RFQ, a true and correct copy of which is attached hereto as **Exhibit J**.

134. Moog made clear that Skyryse's "SoW and inferred technical specification is not mature enough to provide firm pricing." It also expected "a team approach of the SoW, Contract Terms, and specification(s)," showing that this was a completely new and different proposal. It still provided a rough estimate totaling between $47.5M and $75M for 150 shipsets, with $10-15M in design and labor and a unit price of $250-400k for each shipset.

135. In August 2020, Baptist claimed that the unit price for each shipset should be "[redacted]" each for "[redacted]." Thus, based on Skyryse's own statements, its proposed estimate for [redacted] would be between [redacted] at minimum for just the initial shipsets, and not including design and labor costs.

136. After further discussions, on September 22, 2020, Moog provided a further proposal in response to Skyryse's RFQ, this time with a fixed price of $46,195,870, a true and correct copy of which is attached hereto as **Exhibit K**. But, shortly after Moog submitted its bid, Skyryse notified Moog that Moog's proposal was too expensive and Skyryse would be going elsewhere.

137. After it was evident that Moog and Skyryse would not pursue any further business opportunity, there was additional correspondence between the companies about closing up Phase 1. The Parties did not pursue any further business opportunities. Phase 1 concluded, but the terms of the 2018 and 2019

NDAs were never terminated.

138. It was therefore surprising, to say the least, when on October 27, 2021, Skyryse announced a $200 million Series B fundraise in support of its FlightOS product. In the press release, Skyryse's CEO, Mark Groden, proclaimed in the press release that "[t]he general aviation industry is about to change forever."

SKYRYSE'S POACHING OF MOOG EMPLOYEES

139. Notwithstanding the image it presents in its press releases, Skyryse is in the process of pursuing unmanned helicopter aviation in a highly competitive emerging market, one in which approximately twenty (20) companies are racing to become the industry leader by releasing successful, safety-tested, certified, and comprehensive unmanned aviation systems.

140. Before meeting Moog, Skyryse was a "commuter service." After doing limited business with Moog under SOW1, Skyryse became a company focused on developing its own autonomous flight systems and flight control software—projects that Moog had been pursuing since 2012.

141. Facing considerable pressure to meet investor expectations and obtain a significant advantage against competitors, Skyryse made the strategic decision to take what it could not develop quickly enough, and engage in a "full court press" to take from Moog as many key employees as possible so that it could shortcut its own timeline and costs in developing automated flight software and related products.

142. In order to unfairly compete, Skyryse has engaged in a methodical, intentional, and pervasive raid of Moog's developers who built the Stolen Trade Secrets and were familiar and dealt with the Stolen Non-Trade Secret Data. Indeed, the majority of such developers have been poached by Skyryse. And as a result, many of the primary individuals involved in the development, testing, and certification of the Stolen Trade Secrets now work at Skyryse.

143. The following is a list of current and former Moog employees who subsequently worked for Skyryse and have worked on Moog projects intersecting

with the Stolen Trade Secrets and Stolen Non-Trade Secret Data (as well as showing reason for departure, final day at Moog, position, and location):

- Gonzalo Rey – Voluntary termination 8/1/2017; Role: Chief Technology Officer; Location: East Aurora, New York
- Tony Chirico: Retired 9/28/2019; Role: Senior Staff Engineer; Location: East Aurora, New York
- Tim Baptist – Retired 2/29/2020; Role: Group Vice President; Location: Torrance, California
- Robert Alin Pilkington – Voluntary termination 11/12/2021; Role: Sr. Staff Engineer; Location: Torrance, California
- Sathyanarayana Achar: Retired 1/2/2022, Role: Engineering Technical Fellow; Location: Torrance, California
- Nigel Cranwell: Retired 11/1/2021, Role: Electronic Operations Manager; Location: East Aurora, New York
- Eric Chung – Voluntary termination 12/3/2021; Role: Sr. Staff Engineer; Location: Torrance, California
- Misook Kim – Voluntary termination 12/17/2021; Role: Sr. Staff Engineer; Location: Torrance, California
- Lawrence Chow – Voluntary termination 12/17/2021; Role: Software Design Engineer; Location: Torrance, California
- Reid Raithel – Voluntary termination 1/7/2022; Role: PE/NPI Sr. TE Engineering Manager; Location: Torrance, California
- Victor Nicholas – Retired 1/21/2022; Role: Supply Chain Manager; Location: Torrance, California
- Mario Brenes – Voluntary termination 2/5/2022; Role: Software Engineer; Location: Torrance, California
- Cynthia Le – Voluntary termination 2/10/22; Role: Software Engineer; Location: Torrance, California

- Tri Dao – Voluntary termination 2/10/22; Role: Senior Laboratory Engineer; Location: Torrance, California
- Santiago Correa-Mejia – Voluntary termination 2/18/22; Role: Development Engineer; Location: Torrance, California
- Chi Hsin Alex Wang – Voluntary termination 2/20/22; Role: Test Equipment Section Head; Location: Torrance, California
- John Stafford – Voluntary termination 2/25/22; Role: Associate Engineer; Location: Torrance, California
- Alan Lee – Voluntary termination 2/28/22; Role: Development Engineer; Location: Torrance, California
- Dan Gunderson – Voluntary termination 3/4/22; Role: Design Engineer Location: Torrance, California
- Paul Kapuan – Voluntary termination 3/31/22; Role: E1 Sr. Staff Engineer; Location: East Aurora, New York

144. Certain key, senior individuals such as Gonzalo Rey, Sathyanarayana Achar, and Pilkington are extremely familiar with and knowledgeable regarding the Stolen Trade Secrets and Stolen Non-Trade Secret Data, as well as the more capable members of Moog's software engineering teams who worked on these projects.

145. Additionally, several of these individuals hold extremely senior positions within Skyryse where they are in a position to drive the company's strategy and decision making. Tim Baptist, who was formerly a Moog group vice president, is currently Skyryse's Chief Operating Officer (COO). Gonzalo Rey, who was Moog's Chief Technology Officer (CTO), is currently Skyryse's CTO and sits on Skyryse's Board of Directors.

146. Rey, Pilkington and other Skyryse employees, in a strategic effort to carry out Skyryse's raid of Moog, systematically worked to recruit Moog employees to join Skyryse in order to unfairly shortcut development of automated flight software and related products at Skyryse. For example, in August 2021, Gonzalo

Rey attempted to lure Michael Hunter to Skyryse, although Mr. Hunter did not pursue the conversation.

147. For and on behalf of Skyryse, Gonzalo Rey also attempted to poach other Moog employees. For example, Rey also attempted to recruit Todd Schmidt, who resides and works in New York for Moog, to work for Skyryse.

148. On October 13, 2021, Mr. Rey reached out to Todd Schmidt via text message to see if Mr. Schmidt had interest in joining Skyryse. The two spoke on the phone the following day. During the phone call, Mr. Rey walked Mr. Schmidt through what Skyryse was doing, plans for where Skyryse wanted to go, and advised Mr. Schmidt that he would like Mr. Schmidt to join Skyryse.

149. Specifically, Mr. Rey told Mr. Schmidt that Skyryse's goal was extracting flight control functions to an iPad type of interface, the goal being that anyone who can use an iPad can fly a helicopter. Mr. Rey also told Mr. Schmidt that Skyryse wanted to provide an entire system that could fly an aircraft, including software, actuator functions, flight controls, computer hardware, etc. Mr. Rey communicated that Skyryse's grand vision was taking that simplified iPad type of interface to any aircraft—therefore, at some point in the future, any lay person could fly any aircraft using that simplified interface. Mr. Rey told Mr. Schmidt Skyryse's goal was to have a functional product released to the public "within a couple years" and that Skyryse had big investors coming on board to help fund the company's goals. Mr. Rey made it clear to Mr. Schmidt that Skyryse was pursuing all flight control components—software, hardware, and actuation. Thus, it was evident that Skyryse was trying to swiftly re-produce the types of products that Moog had been developing over the course of decades.

150. In connection with the job offer to join Skyryse, Mr. Rey advised that he was looking for a four-year commitment from Mr. Schmidt. He advised Mr. Schmidt that he needed Mr. Schmidt and others to navigate "technical challenges" at Skyryse and to help with FAA certification issues. Mr. Rey told Mr. Schmidt that

he wanted Mr. Schmidt to lead Skyryse's engineering team. While Mr. Rey did not make a specific monetary offer to Mr. Schmidt, he said something to the effect of: "You would become very wealthy." At the conclusion of the telephone conversation, Mr. Schmidt told Mr. Rey that he would consider and get back to him.

151. On October 27, 2021, Mr. Schmidt texted Mr. Rey advising that he was not interested in joining Skyryse for various reasons. Mr. Rey replied and asked if Mr. Schmidt was interested in working remotely, and described other scenarios where Skyryse allowed its staff to work remotely full-time. Mr. Schmidt advised Mr. Rey that he was not interested in joining Skyryse.

152. Pilkington resigned from Moog on November 11, 2021.

153. Once at Skyryse, Pilkington also reached out to Mr. Hunter in or around November 2021 and asked Mr. Hunter to join Skyryse. Mr. Hunter resides in and works in New York for Moog. Pilkington later told Mr. Hunter there was "urgency" at Skyryse. Mr. Hunter declined Mr. Pilkington's offer.

154. On November 15, 2021, Deb Morisie (Head of People at Skyryse) called Moog's Software Chief Engineer Jorge Lopez and offered him a job at Skyryse. Later that day, Ms. Morisie texted Mr. Lopez asking to set up a further call. On November 17, 2021, Mr. Lopez advised Ms. Morisie via text that he would not be pursuing a potential job opportunity at Skyryse.

155. Kim left Moog to join Skyryse on or about December 18, 2021.

156. Skyryse has reached out to a large number of software engineers at Moog who worked on the Moog projects that intersect with the Stolen Trade Secrets and Stolen Non-Trade Secret Data in the United States, primarily targeted at Moog's Los Angeles-area office.

157. Even after the filing of this lawsuit on March 7, 2022, Skyryse and/or individuals on Skyryse's behalf continued to contact, solicit, and recruit Moog personnel.

158. To date, Skyryse has hired twenty (20) former Moog employees, and

has solicited many more. All of these former Moog software employees had substantial and direct involvement in the building, testing, and certification of the projects reflected in the Stolen Trade Secrets. For example, in Moog's Los Angeles-area office, there were nine (9) developers who could write software code. Five (5) out of these nine (9) developers have left Moog to join Skyryse.

MASSIVE THEFT AND MISAPPROPRIATION OF MOOG'S CONFIDENTIAL, PROPRIETARY AND TRADE SECRET INFORMATION

159. Suspecting that Skyryse was engaged in an all-out raid of its flight software employees based on an increasing level of resignations and departures to Skyryse, in late January 2022, Moog had its Security Operations team look into whether individuals who had left Moog for Skyryse, or were soon leaving Moog to join Skyryse, had taken or copied any Moog data before their departure.

160. As explained elsewhere herein, misappropriating and stealing Moog's developed proprietary and trade secret information would provide to Skyryse significant competitive advantages.

161. Moog's Security Operations team conducted an investigation into the user accounts and data activity associated with former employees at Moog who had recently departed Moog to begin working for Skyryse.

162. Using those employees' user names and an endpoint policy enforcement solution software product, Moog investigated which files had been downloaded or copied from Moog's internal servers onto removable devices (i.e., external hard drives, USB devices, etc.).

Theft and Misappropriation by Misook Kim

163. Moog's security investigation revealed that, while still a Moog employee, on November 19, 2021, Kim copied a significant volume of data from Moog's internal servers to an external hard drive, amounting to greater than 136,000 files, less than one month before her last day at Moog, and less than one week after Pilkington, her supervisor, left Moog for Skyryse on November 12, 2021. All of the

data copied by Kim is located on Moog's central servers in East Aurora, New York.

164. The data Moog was able to gather from Kim's electronic devices and Moog user profile include: (1) timestamps of when she used her removable devices; (2) the identifying credentials and specification of the devices that were used in the data copying; (3) the names and types of the data files that were copied over; and (4) the directory structure and file path used in connection with the copying.

165. The timestamps for Kim's user account show that the unauthorized copying of Moog internal server data to the external hard drive was conducted via Virtual Private Network ("VPN") on Friday, November 19, 2021 between 3:16 a.m. and 7:33 a.m. local time in California. Kim's normal working hours on weekdays were 8:00 a.m. to 5:00 p.m. in Moog's Torrance, California offices. Because the download occurred via VPN, upon information and belief, Kim downloaded Moog's data from her home or other remote location. Further, the time of day when Kim copied Moog's data made it easier for her to escape detection.

166. Moog investigated the data that was copied by Kim, and prepared a file log for the copied data (the "File Log"), which showed that Kim copied a total of 136,994 files, consisting of:

- 43,960 source code files;
- 5,377 spreadsheets;
- 2,831 document files;
- 954 executable files;
- 9,003 image files;
- 2,010 MAP files;
- 7,898 model files;
- 1,026 object files;
- 4,613 plain text files;
- 404 presentation files;
- 20,655 miscellaneous files; and

- 38,263 SVN logs.

167. The data copied by Kim includes nearly all of the source code, documentation, and related information regarding the composition, testing, and certification of Platform and project-specific applications.

168. Moog's review of the File Log showed that the following program classifications were found (showing which program data and code had been copied by Kim):

- AMP
- Sensitive Government Program 1
- EHFCAS
- eRTOS
- G280
- Platform
- Sensitive Government Program 2
- Software Engineering Process
- TERN
- V280
- X47B

169. Moog's review of the File Log confirmed that the entire application layer for Platform was copied by Kim, meaning that 100% of the base Platform software and its code were copied.

170. Platform, eRTOS, and AMP were copied, as well as test artifacts related to some of the iterations.

171. In addition to the Platform base software, the data and code for several project-specific applications were also copied, as reflected above. This includes several military programs. Kim copied all 76 of Moog's software checklists as well as other documents from its checklist repository. Kim essentially copied a substantial amount of Moog's flight control software engineering development

efforts up through the time of the theft.

172. Each employee working on Moog's projects had their own "branch" or location on Moog's server, where they could store sensitive materials they needed to access to as part of their work.

173. Moog's investigation of the File Log shows that Kim used Pilkington's branch to copy the data onto the external hard drive. As detailed below, there was no reason for Kim to access the data in this fashion, let alone copy it, aside from being directed to do so by Pilkington and Skyryse ahead of her resignation from Moog. This was not accidental, or merely incidental to some legitimate work activity for Moog.

174. Indeed, the file path used by Kim to copy Moog's data was: "D:\Misook\ENG_Alin_Branch\Software . . . ." The file path thus shows that Kim went into Pilkington's branch and copied everything that Pilkington worked on under that branch, as well as substantial additional materials that both Kim and Pilkington had access to during their employment at Moog.

175. Importantly, while Kim had credentials to use her own file path, on which much of the same data was stored including the Platform base software, she instead used Pilkington's file path. This is because she was guided and/or assisted by Pilkington in identifying what files to download. Pilkington had intimate knowledge of what files were stored on his file path.

176. Kim copied the data onto an external hard drive which was issued to her by Moog, and she did not return it upon her departure from Moog. As described further below, the hard drive was only returned later to Moog several months later after demand by Moog for its return, and the hard drive was completely wiped clean.

177. Kim signed an exit form (the "Exit Form") on her last day at Moog, December 17, 2021, a true and correct copy of which is attached hereto as **Exhibit L**. Therein, Kim affirmed in writing that she had returned all Moog "TRADE SECRET/COMPANY CONFIDENTIAL INFO." The Exit Form also states that: 1)

Kim was "provided access to [Moog's] proprietary information"; 2) she "owes a fiduciary duty to Moog to not usurp any such corporate opportunity for [her] own benefit"; 3) "use of proprietary information of Moog by [Kim] . . . would be pursued by Moog using all available means;" 4) Kim affirms that she does "not maintain access to, or have possession of, any tangible or digital record of Moog IP-whether in hard copy or digital form—on any device, cloud, or digital storage facilities." Clearly, Kim did not abide by her contractual obligations on many accounts.

178. Exit form aside, the standard way in which Moog employees worked on Moog's trade secrets would have been to connect to the Moog server via virtual private network ("VPN") and access data that way. All of the data copied by Kim is located on Moog's internal servers. Even if Kim was working on a different Moog computer, she could have easily accessed all the data she copied from Moog's Subversion network using her own login credentials and branch. Even if downloading data was necessary (which it was not), a copy of the data would be stored to the user's hard drive on their Moog laptop computer – not an external hard drive.

179. Further, at the time of her departure in December 2021, Kim was working solely on "Sensitive Government Program 2." Kim was a software testing engineer, not a code-writer. Thus, even if Kim wanted to access certain Moog data for legitimate business purposes, she would only have a need to access certain verification and testing data related to Sensitive Government Program 2 (instead of the entire application layer for several projects she never touched). To support legitimate business purposes, Kim would have needed, at most, to access 0.5% of the total data that she copied on November 19, 2021. The discrepancy speaks for itself.

180. When Moog discovered Kim's theft, Moog was not aware of any precedent to what Kim did. At the time, Moog was aware of no other instance where a Moog employee copied to an external hard drive even a fraction of the data

that Kim did in November 2021. However, as explained further below, Moog later learned that Pilkington's theft was *exponentially greater*.

Kim Returns Two Hard Drives, Wiped Completely Clean

181. On January 28, 2022, Moog requested that Kim return the company-issued external hard drive she had in her possession. On January 31, 2022, Kim's sister who also works at Moog returned on Kim's behalf a hard drive to Moog. However, an initial inspection of this device, a Western Digital My Passport drive (the "Western Digital Hard Drive"), revealed it was not the external hard drive device Kim had used to copy Moog's data on November 19, 2021, ***and*** it had been completely wiped clean.

182. On February 18, 2022, Moog sent a further letter to Kim demanding that she return the external hard drive in question. In response, Kim called Moog's HR employee Jamie Daly, and stated she had possession of the Moog external hard drive, had used it to download a large set of files purportedly to help other Moog employees after her departure, and that she had erased all the files from the drive. This explanation made no sense. Kim had no reason to take the unprecedented step of downloading nearly 137,000 files, the vast majority of which she had never worked on and had no use for at any time in her employment at Moog, let alone the final few weeks. No other employees indicated that they would need to continue working with Kim or needed her to maintain possession of the utmost secure and sensitive data after her time at Moog, let alone while working for competitor Skyryse. Nor would her job duties as an engineering tester have reasonably led to her needing to reference or transmit any of this data in the course of her transition out of Moog. And, Kim signed the Exit Form where she affirmed that she had returned all confidential data to Moog and would not retain any copies.

183. When Kim eventually returned the second hard drive, a SAMSUNG T7 series, model MU-PC1T0H, serial number S5SXNS0R702326Z, (the "Samsung 1 Hard Drive") to Moog on February 21, 2022, an initial inspection confirmed it had

been wiped before being returned. An official forensic inspection revealed the situation to be much worse.

Forensic Analysis of Kim's External Hard Drives and Laptop Devices Reveals Deliberate Data Wiping and Additional Theft

184. Bruce W. Pixley, an expert computer forensic examiner with more than 20 years of experience, performed an official forensic analysis of true and correct bit-for-bit copies of the Western Digital and Samsung Hard Drives returned by Kim, as well as her two Moog-issued laptop devices ("Dell Laptop 1" and "Dell Laptop 2"). He also reviewed the File Log.

185. First, Mr. Pixley's analysis confirmed that Kim had indeed copied 136,994 files of Moog's data on November 19, 2021 between the hours of 3:34 a.m. to 7:33 a.m. PST from Dell Laptop 1 to the Samsung Hard Drive. When Kim copied these files, they were copied to a sub-folder on the Samsung Hard Drive called "Misook."

186. Second, Mr. Pixley's analysis revealed that the "Misook" folder on the same Samsung Hard Drive was intact when it was connected to Dell Laptop 2 on December 15, 2021. On this same date, a new folder was added to the Samsung Hard Drive called "OneNote Notebooks." Microsoft OneNote is a program that is used to store user's notes, drawings, and screen shots. In searching Dell Laptop 2, Mr. Pixley discovered that a folder called "OneNote Notebooks" had been stored in Kim's Documents folder, containing over 200 digital notebook files. However, on December 17, 2021, Kim's last day at Moog, the entire "Misook" folder on Dell Laptop 2 was deleted in its entirety. The deleted "Misook" folder contained approximately 54 GB of data. Mr. Pixley's analysis reveals that this was an intentional user deletion of data and the data was not transferred to the user's Recycle Bin folder where it could be easily recovered.

187. The OneNote files contained Kim's workbooks created over her years of employment at Moog, and include information helpful to her in utilizing the

improperly downloaded data files she took.

188. Third, and perhaps most importantly, Mr. Pixley's analysis reveals that the Samsung 1 Hard Drive (which was used to copy 136,994 files on November 19, 2021 and additional notebook data on December 15, 2021) was intentionally formatted sometime after Kim's departure from Moog on December 17, 2021 and before it was returned on February 21, 2022. When a hard drive is formatted, it needs to be connected to a computer. Mr. Pixley determined that at the start of the formatting process, an option was used that forced the formatting process to overwrite all sectors on the drive with zeroes. Therefore, not only was this formatting of the Samsung Hard Drive an intentional act, but this specific formatting process effectively wiped all previous data on the drive so it would be unrecoverable. This formatting prevents any ability to see the data that was erased on the Samsung Hard Drive. It also prevents any ability to determine whether, when, how, or to where any of the underlying data on the Samsung 1 Hard Drive was copied, transferred, or otherwise exported to another device.

189. Fourth, Mr. Pixley determined that the Samsung 1 Hard Drive had a volume name of "Misook-T7." The volume name for the Western Digital Hard Drive (the initial false hard drive that was returned to Moog) had been intentionally changed from its factory default name to "Misook T7," in an apparent attempt to resemble the Samsung 1 Hard Drive that was actually used to copy Moog's data on November 19, 2021 and December 15, 2021.

190. Mr. Pixley's analysis also revealed that a ***third*** external hard drive was connected to one of Kim's laptops several times on September 27 and 28, 2021, and November 22, 28, and 29, 2021. This third external hard drive was a second Samsung USB solid state storage device, Series T7, serial number S5SXNS0R700159M ("Samsung 2 Hard Drive"). At the time of the filing of the initial Complaint, the Samsung 2 Hard Drive had not been returned or otherwise made available to Moog, but has since been made available to Moog through the

parties' neutral forensic vendor iDS. As Moog discovered through its inspection of that device, and as explained further below, the Samsung 2 Hard Drive had been used by Pilkington to copy significant additional files from Moog.

191. Finally, an inspection of Kim's two Moog-issued laptop devices indicates that the back covers of the laptops have been removed because the screws were not "factory tight." The laptops' hard drives can be easily accessed and removed by removing the back cover of the laptops.

192. In short, Kim, in concert with Defendants, stole large volumes of Moog's confidential and proprietary data on multiple occasions, used a number of devices and re-named them to avoid detection, and deliberately formatted and deleted the data such that Moog cannot follow the trail of what happened to its stolen data. Moog does not have possession of the files that Kim permanently deleted (because they were permanently deleted). While Moog has attempted to find approximate matches of what Kim permanently deleted from elsewhere in Moog's systems and devices, some of the data Kim permanently deleted is unique such that Moog cannot even find an approximation. Because of Kim's permanent deletions and other related conduct, Moog has been precluded from possessing or using various Moog files that Kim stole. This conduct speaks for itself.

Theft and Misappropriation by Pilkington

193. When this lawsuit was initially filed on March 7, 2022, and while its investigation was ongoing, Moog was only aware of the 136,994 files taken by Kim. But this was just the tip of the iceberg. ***The total number of stolen Moog files in this case now exceeds 1.4 million***.

194. On September 9, 2021, Pilkington created a user profile on his Moog laptop. On September 10, 2021, Pilkington connected Samsung 2 Hard Drive to his Moog laptop. As described above, this is the same hard drive that was connected to Kim's Moog laptop just a few weeks later on September 27, 2021. On September 10, 2021, Pilkington copied data to the Samsung 2 Hard Drive using the file path

"C:/MoogPrograms."

195. On September 11, 16, 17, and 21, 2021, Pilkington again connected the Samsung 2 Hard Drive to his Moog laptop and accessed different folders on the hard drive. Based on file path information available to Moog, some of the folders accessed by Pilkington on these dates included folders related to Emerald and Sensitive Government Program 2, as well as Python scripts and other source code documents.

196. On September 27 and 30, 2021, Pilkington again connected the Samsung 2 Hard Drive to his Moog laptop and copied Moog data to the hard drive. The file paths associated with these acts of copying include "D:\LL Folders\Alin\LL (9-27-2021)\" and "D:\LL Folders\Alin\LL (9-30-2021)\". These activities overlap with Kim also connecting the Samsung 2 Hard Drive to her Moog laptop on September 27 and 28, 2021.

197. On October 27, 2021 (the date that Pilkington provided notice of his resignation from Moog), Pilkington connected a new and separate Buffalo SSD-PGU3 1 TB external hard drive (the "Buffalo Drive") to his Moog laptop. On that date, Pilkington copied approximately 1.1 million files of Moog proprietary and confidential data from his Moog-issued laptop onto the Buffalo Drive. Based on file path information available to Moog, one of the file paths used to copy the Moog data include "D:\C\Users\apilking\". This indicates that Pilkington copied essentially every Moog document related to Moog's Toolsets and Programs that he had access to while at Moog.

198. On November 11, 2021, Pilkington connected the Samsung 2 Hard Drive and copied additional Moog data to the hard drive. Based on file path information available to Moog, the data copied by Pilkington included data relating to Sensitive Government Program 2 and eRTOS.

199. Then, on November 12, 2021 (Pilkington's last day at Moog), Pilkington copied an approximately 130,000 additional files of Moog proprietary

and confidential data from his Moog-issued laptop onto the Buffalo Drive.

200. A forensic analysis of the Buffalo Drive and Samsung 2 Hard Drive confirms that Pilkington copied at least 1.2 million Moog files to the hard drives. The data copied by Pilkington generally includes the data copied by Kim, but of course contains far more data than was copied by Kim. Pilkington copied a substantial amount of trade secret and proprietary data from Moog, including the Stolen Trade Secrets described above in Paragraphs 31 through 45.

Theft and Misappropriation by Reid Raithel

201. During his last week of employment at Moog, former Moog employee and subsequent Skyryse employee Reid Raithel plugged in two Samsung USB drives into his Moog laptop ("USB Drive 1" and "USB Drive 2"). He copied 27,118 files from USB Drive 1 to USB Drive 2. He also copied certain files from his Moog laptop to USB Drive 2. Upon his departure from Moog, Raithel left USB Drive 1 behind with Moog. However, he never returned USB Drive 2 to Moog.

202. Approximately 13,011 of these files reflect trade secret material. The materials copied by Raithel includes [redacted]

203. One of the 27,118 files copied by Raithel has a file name of "Listing new.xlsx" (Author: Raithel; Created: 1/4/2022; Company: Moog Inc.), and it was copied to USB Drive 2 which was connected to Raithel's Moog laptop on January 4, 2022. This document appears to be a recruiting list of targeted Moog employees. Raithel deleted this file to his Recycle Bin on his Moog laptop on January 6, 2022, just before he departed Moog employment to join Skyryse.

204. On January 29, 2022, Raithel (using his Skyryse e-mail account) sent an e-mail containing one attachment, an Excel spreadsheet called "[redacted]

[redacted]." The Excel metadata shows the same metadata as for the file "Listing new.xlsx." The e-mail was sent to the Skyryse e-mail addresses for Deb Morisie, Jeff Becker, and Sathya Achar. Achar forwarded this e-mail and attachment to Pilkington's Skyryse e-mail account on January 31, 2022. Thus, Raithel evidently used a targeted list of Moog employees that he took from Moog over to Skyryse to further Skyryse's efforts to solicit and raid Moog's employees.

Theft by Eric Chung

205. Pilkington's Moog laptop contained several different Requirements Based Test (RBT) spreadsheets. The RBT Spreadsheet is a custom-formatted Excel spreadsheet, which provides the necessary information for running a software test.

206. There were at least 100 and unique (non-duplicates) RBT Spreadsheets on Pilkington's Moog Laptop that contained all or some of the following attributes:

- All of these RBT Spreadsheets had the same metadata for file creation date, which was 6/5/2015, when Pilkington was employed at Moog.
- 96 of these RBT Spreadsheets files had the same metadata for author, which was Eric Chung and four were blank; and
- 22 of these RBT Spreadsheets contained a print header with the text "DO NOT TRANSMIT OUTSIDE OF MOOG USA OR TO Non-U.S. PERSONS*."

Based on these 100 RBT Spreadsheets, it appeared that these files started as one template originally created on 6/5/2015 and saved with different content as needed for each test.

207. Chung's Skyryse Laptop contains an RBT Spreadsheet, and the original author metadata shows that it was created by Eric Chung on 6/5/2015, which is when Eric Chung worked at Moog, and was last modified on 3/6/2022. The formatting of this RBT Spreadsheet was consistent with the RBT Spreadsheets located on Pilkington's Moog Laptop.

208. Chung's Skyryse's Laptop contains 11 different versions of the RBT

Spreadsheets, which had the same metadata creation date of 6/5/2015 and were all last modified in 2022. Three of the 11 versions contained print header information that displayed "*DO NOT TRANSMIT OUTSIDE OF MOOG USA OR TO Non-U.S. PERSONS*." One of the 11 versions showed Skyryse employee Mario Brenes as the author with an original metadata creation date of 6/5/2015. Thus, Chung accessed and used stolen Moog files while at Skyryse.

Theft by Tri Dao

209. On February 6 and February 9, 2021, while employed at Moog, Dao copied 39,278 files to an external USB drive (240 GB, USB serial number 30000000123ada). This external USB drive has not been returned to Moog.

210. Approximately one week later on February 15, 2021, Tri Dao plugged that same external USB drive into his Skyryse laptop and copied 7,679 files (of the 39,278 files) he originally copied from his Moog laptop to his Skyryse laptop.

211. Because Moog does not have access to the external USB drive or Dao's laptop (despite having sought it from Skyryse), it cannot yet determine the nature and extent of Tri Dao's theft and misappropriation of Moog's trade secrets and other proprietary data.

Possession and Use of Moog Data by Sathya Achar

212. An inspection of Achar's Skyryse laptop reveals that it contains at least 81 Office-type documents (Word, Excel, PowerPoint) that reflect "Moog Inc." or "Moog" in the company metadata field; one PDF document that contained the line "MOOG PROPRIETARY AND CONFIDENTIAL INFORMATION"; and 173 PDF documents that contained one of the following lines of text: "Material licensed to Moog Inc;" "Sold to MOOG INC;" "Downloaded by Moog Inc;" and, "Issued to Moog Inc."

213. Thus, Achar possessed and/or used Moog trade secrets or other non-public information while at Skyryse.

Theft by Lori Bird

214. Lori Bird is a former Manager Software QA Assurance at Moog. She worked out of Moog's Salt Lake City, Utah offices. Bird's employment with Moog ended on February 8, 2020. She then served as a contractor for Moog until September 29, 2021. Around the same time when Pilkington and Kim joined Skyryse, Bird then became a contractor or employee for Skyryse, upon which she received and used a Skyryse e-mail account and a Skyryse-issued computer. Bird frequently possessed, received, accessed, transmitted, and used Stolen Trade Secrets and Stolen Non-Trade Secret Data (including proprietary source code documents and software development checklists and templates) during her tenure at Skyryse, including using her Skyryse e-mail account and Skyryse laptop.

215. For example, On December 18, 2021, Pilkington (while employed by Skyryse), e-mailed Bird no less than ***89 documents*** comprising Moog proprietary software checklists, standards, development plans, and other related documents. Most of these documents contain "Moog" on the document or metadata, and some of them have explicit Moog legends that they comprise "MOOG PROPRIETARY AND CONFIDENTIAL INFORMATION."

216. In December 2021, Bird exchanged a series of text messages with Pilkington discussing the misappropriation and use of proprietary Moog data for Skyryse purposes. For example:

- On December 13, 2021, Bird asks Pilkington: [redacted]

It is evident that multiple Skyryse personnel stole, used, and referenced Moog

software templates and checklists, evidently because Skyryse did not have such templates and was starting from zero.

- In the same thread, Bird asks Mr. Pilkington if he would like her to get "SQA checklists," to which Pilkington responds: "I may have them too. Would they be in the [Sensitive Government 2] or [Sensitive Government 1] project?" Pilkington asks Bird to provide "the paths."
- In a similar thread, Bird advises Pilkington: [redacted]
- As another example, in the same thread Bird asks Pilkington: [redacted]

As described further below, Bird frequently and repeatedly used and disclosed to third parties the Stolen Trade Secrets and Stolen Non-Trade Secret Data.

217. Moog has recently discovered that shortly after leaving Moog, Bird communicated with former Moog employee Kathy Stone and caused her to send Bird proprietary Moog DPA Checklists. For example, on November 9, 2022, Bird asked Stone via phone chat message: "[redacted]"? In response, Stone responded "[redacted]" following by "[redacted]." On November 15, 2022, Stone communicated with Bird via phone chat message, and stated: "[redacted]." On November 22, 2022, Bird again asked Stone via chat message: "[redacted]"? Stone responded: "[redacted]." Stone ultimately sent to Bird certain proprietary Moog DPA review checklists.

218. After this lawsuit was filed, Bird and Stone exchanged additional chat messages about Moog DPA checklists. Bird advised Stone via chat message: "[redacted]." Stone responded: "[redacted]." Evidently, both Bird and Stone were aware that Moog's DPA checklists were proprietary and that disclosure outside of Moog was not permitted. This is made clear by Stone not wanting to "[redacted]" or "[redacted]." Stone has been terminated by Moog.

Skyryse's Unauthorized Possession and Disclosure of Moog's Trade Secrets and Proprietary Information

219. There is substantial evidence that Skyryse personnel possessed, used, and disclosed to third parties the Stolen Trade Secrets and Stolen Non-Trade Secret Data without Moog's authorization. In terms of disclosure to third parties, Skyryse personnel frequently disclosed Moog's trade secrets and non-public information to various personnel at third party Hummingbird Aero, LLC ("Hummingbird"), an aviation contractor.

220. Select examples of Skyryse's misappropriation and unauthorized possession, use, and disclosure of the Stolen Trade Secrets and Stolen Non-Trade Secret Data are as follows:

- On March 31, 2021, Skyryse personnel Hussein Khimji (using a Skyryse email address) sent an email to both Skyryse and Hummingbird employees that contained an attached Plan for Software Aspects of Certification (PSAC) template document with "Moog" in the document metadata.
- On May 26, 2021, Hussein Khimji (using a Skyryse email address) sent an email to both Skyryse and Hummingbird employees that contained an attached PSAC template document with "Moog" in the document metadata.
- On November 18, 2021, Bird (using a Skyryse e-mail address) sent an email to Hummingbird employees containing 16 attachments (HB0000700). These attachments are all nearly identical to corresponding Moog templates and

checklists found on Pilkington's Moog laptop, and the files matched by similar file name. Three of these attachments have "Moog" in the text of the document.

- In an email sent on November 18, 2021, Bird (using her lori.bird@skyryse.com e-mail account) sent Hummingbird personnel Rex Hyde and Jonathan Lynch an email that states, "[redacted]." Attached to this email are 3 Word documents and 13 Excel spreadsheets, which are visually identical to corresponding Moog Data Processing Agreement (DPA) checklist documents.
- On November 22, 2021, Bird (using her Skyryse e-mail address) sent an email to Hummingbird personnel Rex Hyde and Jonathan Lynch containing 20 attachments. In her cover e-mail, she notes: "[redacted]." These documents are all nearly identical to corresponding Moog checklists found on Pilkington's Moog laptop, and the files matched by file name. Five of these attachments have "Moog" in the text of the document.
- Bird frequently communicated with other Skyryse personnel and Hummingbird personnel about possessing, transferring, and using Moog trade secrets and non-public information at Skyryse. For example, in an email sent on December 17, 2021, Bird (using her lori.bird@skyryse.com e-mail address) asks Hummingbird personnel Rex Hyde from Hummingbird: "[redacted]"
- Again on December 17, 2021, Bird (using her lori.bird@skyryse.com e-mail address) also sent former Skyryse employee Pilkington an email that states, "[redacted]." The

documents that Lori Bird is requesting provide detailed instructions on how to use JIRA and SVN in the Moog configuration management system.

- Additional emails are sent on December 19, 2021 by Bird (using her lori.bird@skyryse.com e-mail address) to Hummingbird personnel Rex Hyde and former Skyryse employee Pilkington, continuing to ask for Moog documents. Pilkington responds with "Text me in an hour when I'm home and I'll find something." The referenced Moog documents are ultimately sent to Bird's Skyryse email as attachments by Rex Hyde from his Hummingbird email on December 19, 2021: 1) [redacted]; and 2) [redacted]. The title pages of these documents have a legend that states "MOOG PROPRIETARY AND CONFIDENTIAL INFORMATION This technical Data/Drawing/Document contains information that is proprietary to, and is the express property of Moog Inc., or Moog Inc. subsidiaries except as expressly granted by contract or by operation of law and is restricted to use by only Moog employees and other persons authorized in writing by Moog or as expressly granted by contract or by operation of law. No portion of this Data/Drawing/Document shall be reproduced or disclosed or copied or furnished in whole or in part to others or used by others for any purpose whatsoever except as specifically authorized in writing of Moog Inc. or Moog Inc. subsidiary."
- On January 6, 2022, Bird (using a Skyryse e-mail address) sent an email to David Berlin (Hummingbird email address) attaching two software code checklists. Both of these checklists are nearly identical to corresponding Moog checklists and the company metadata field for both documents is "MOOG Salt Lake Operations."
- On February 1, 2022, Bird (using her lori.bird@skyryse.com e-mail account) sent an e-mail to various Skyryse and Hummingbird personnel requesting

comments on "[redacted]". Two of the attached software checklists are Moog checklist templates with "MOOG Salt Lake Operations" in the Company metadata.

- In an email sent on March 11, 2022, Bird (using her lori.bird@skyryse.com e-mail account) sends Hummingbird personnel Matt Neffinger an email with the subject "[redacted]" and attaches 9 Word documents. These Word documents comprise the Skyryse software plans and standards for the Skyryse Flight OS. Portions of many of these documents (including Skyryse's SCMP, SDP, and SQAP) are derived from corresponding Moog documents and templates.
- On June 8, 2022, Bird (using her lori.bird@skyryse.com e-mail account) sends an email to Hummingbird personnel indicating that she has asked David Nguyen (Skyryse's Designated Engineering Representative (DER)) to schedule their SOI 1 audit (an activity in which the certification authority reviews the applicant's software planning documents) on 6/23/22. Attached to this email are 5 Word files which comprise most of the Skyryse software planning documents. For this audit to occur, Skyryse must baseline and formalize their software process using these documents. Three of the documents attached to this email are based on the Moog templates.

221. The Skyryse personnel and e-mail accounts that are implicated in the unauthorized possession, use and disclosure of Moog's trade secrets and non-public information (including disclosure to Hummingbird personnel) include:

- Alin Pilkington <alin.pilkington@skyryse.com>
- Amir Hallajpour <amir.hallajpour@skyryse.com>
- Chris Smith <chris.smith@skyryse.com>
- David Lee <david.lee@skyryse.com>
- Diane Li <diane.li@skyryse.com>
- Gonzalo Rey <gonzalo.rey@skyryse.com>

- Hussein Khimji <hussein@skyryse.com>
- Ian Young <ian-a@skyryse.com>
- Lawrence Chow <lawrence.chow@skyryse.com>
- Lori Bird <lori.bird@skyryse.com>
- Mario Brenes <mario.brenes@skyryse.com>
- Norman Butler <norman.butler@skyryse.com>
- Paul Kapaun <paul.kapaun@skyryse.com>
- Reid Raithel <reid.raithel@skyryse.com>
- Sathya Achar <sathya.achar@skyryse.com>
- Stephen Wang <stephen.wang@skyryse.com>
- Ilan Paz <ilan.paz@skyryse.com>
- Thusa Dinh <thusa.dinh@skyryse.com>
- Glenn Shintaku <glenn.shintaku@skyryse.com>

222. The Hummingbird personnel that are implicated in the unauthorized possession, use and disclosure of Moog's trade secrets and non-public are as follows:

- Rex Hyde
- Dave Manzanares
- Brian Barker
- John Harris
- Rory Kaclik
- Jonathan Lynch
- Phil Gillaspy
- David Berlin
- Matt Neffinger
- Gordon Burger
- Deon Esterhuizen
- Shawn Taylor

- Dominic D'Souza
- Josh Brashears
- Jon Nesbitt
- James Monczynski
- Steve Wolgamott
- Waseem Wahba

Skyryse's Use of the Stolen Trade Secrets and Stolen Non-Trade Secret Data

223. Skyryse did not just possess and disclose Moog's trade secrets and proprietary information on a large scale, as described above. Skyryse also did not just discuss using Moog's trade secrets and proprietary information. Rather, there is voluminous specific, detailed evidence that Skyryse personnel have used and incorporated Moog's trade secrets and proprietary information into Skyryse's software, checklists, and certification plans. Skyryse personnel did much more than just copy Moog data—they altered and modified Moog documents for internal use at Skyryse. Moog has therefore been prevented from exclusive possession and use of its own confidential and proprietary data. In addition to the foregoing examples, select additional examples of Skyryse's unauthorized use of Moog's trade secrets and non-public information are as follows:

- A Moog document, [redacted], became the foundation of the Skyryse document [redacted]. Bird sent this to several Skyryse and Hummingbird email addresses on January 5, 2022. The Skyryse document has nearly identical structure and numerous identical word-for-word passages as the Moog document. The Moog document was also incorporated into [redacted].
- Skyryse's [redacted], dated December 3, 2021, is based on the Moog PSAC template. Usage of the Moog template is evident in the nearly identical document structures

and numerous copied word-for-word passages. This document was continuously edited and revised by Lori Bird and various Skyryse personnel, and it was sent to numerous Skyryse and Hummingbird personnel from at least December 2021 to June 2022.

- Skyryse's [redacted] was sent to Pilkington by Bird (using her Skyryse e-mail account) on January 10, 2022. This document is nearly identical to the Moog SQAP. This is evident in the nearly identical document structures and numerous copied word-for-word passages. This document was continuously edited and revised by Bird and was sent to numerous Skyryse and Hummingbird personnel from at least December 2021 to June 2022.
- Skyryse's [redacted] is nearly identical to the Moog SCMP template. These documents contain nearly identical document structures and numerous copied word-for-word passages. The Skyryse document includes references to [redacted] This is a tool used by Moog for requirements management and change control. This Skyryse document was continuously edited and revised by Bird and was sent to numerous Skyryse and Hummingbird personnel from at least December 2021 to June 2022.
- Skyryse's [redacted] is derived from the Moog SDP template. This document retains the structure and numerous word-for-word passages of the Moog template. This document was continuously edited and revised by Bird and various Skyryse personnel and was sent to numerous Skyryse and Hummingbird personnel from at least December 2021 to June 2022.

224. As described above, Skyryse based their software plans on Moog templates. They continuously updated and revised these plans from December 2021

through at least June 2022. On June 7, 2022, Bird (using a Skyryse e-mail account) sent Skyryse personnel Thusa Dinh, David Lee, and Glenn Shintaku, and Designated Engineering Representative (DER) David Nguyen, various software plan and checklist templates. The thread shows that Bird asked Nguyen about Skyryse's Stage of Involvement (SOI) 1 on June 23, 2022. SOI 1 generally comprises a planning audit where the DER would audit Skyryse's software planning documents (such as PSAC, SDP, SVP, SCMP, SQAP, and standards). Three of the documents attached to this email, [redacted], have been shown in detail above to be derived from Moog templates.

225. On or about July 11, 2022 Skyryse management personnel approved these plans. With this approval, these plans become the formal guidance for the methods and procedures the Skyryse software team would use to develop software and cannot be changed without following the formal change procedure detailed in the SCMP. This formally incorporated many portions of the Moog software engineering process into the Skyryse software process, thus furthering the use and reliance on Moog trade secrets and non-public data.

226. During the relevant time periods, both Skyryse and its DER David Nguyen were aware that Skyryse was using Moog templates without authorization. For example, in providing comments on a Skyryse software certification plan, Nguyen noted: "[redacted]"

THE DEFENDANTS' ACTIONS HAVE CAUSED AND CONTINUE TO CAUSE IRREPARABLE HARM TO MOOG

227. Defendants' intentional and sweeping misappropriation and theft of Moog's confidential, proprietary, and trade secret information and intentional and orchestrated raid of Moog's software developer employee team to unfairly compete and exploit Moog's confidential, proprietary, and trade secret information have caused, and continue to cause, substantial and irreparable harm to Moog.

228. Unmanned helicopter aviation, which Moog is pursuing and understands Skyryse is also pursuing, is a new market. There is no established market and no industry leader yet. About twenty (20) companies, including Moog and Skyryse, have entered the market and are rushing to become the market leader. Whichever company wins that race will likely win a large portion of the market share just by being the first to market with a viable product. If another party gained access to Moog's trade secrets and other proprietary information, it would give that party a substantial and unfair competitive advantage as it would save that party literally many millions of dollars and several years investing in development and testing that software. Moog has invested approximately eleven (11) years of research and development into automated flight technologies and sixteen (16) years in developing the trade secrets at issue. As noted, these Toolsets, Programs, and other trade secrets take many years to build, test, and certify. By stealing Moog's source code and other proprietary information reflected in the Stolen Trade Secrets as well as the Stolen Non-Trade Secret Data, and crippling Moog's software engineering workforce, Skyryse has jumped to the front of this race to be first to market and has slashed Moog's tires along the way. This race against time underscores the irreparable harm faced by Moog because time cannot be unwound.

229. Skyryse has demonstrated that it will do whatever it takes (no matter how unlawful or unethical) to be first to market. Multiple Hummingbird engineers who were working on Skyryse projects quit their employment with Hummingbird because they "[redacted]." The theft of the Stolen Trade Secrets and Stolen Non-Trade Secret Data to fast-track its software development is emblematic of Skyryse's approach and conduct.

230. Part of what makes Moog unique and competitive in the marketplace is that it can put entire systems for aircraft flight control (*i.e.*, software and hardware) together in-house. Most other competitors can only do one or the other. Moog

builds software and hardware components safely through the use of architectural diagrams.

231. Importantly, there is a high barrier to entry in the flight control software market. Companies that have an established, tested, and proven software and have successfully delivered on contracts before have a huge advantage in securing contracts from the government and other third parties. Moog's trade secrets provide Moog with that competitive advantage. Contracting parties understand that because of Moog's Toolsets (including Platform) and other proprietary data, it will be faster and less expensive to tailor its flight control software to a particular aircraft because the substantial foundation has already been built.

232. On information and belief, other companies would have to pay two to three times what Moog does because Moog has an established flight control operating system software. As a result, Moog wins many of the flight control projects that it bids on.

233. Kim, Pilkington, and other Skyryse personnel copied essentially all of Moog's source code and other underlying data for 5 Toolsets and 21 commercial and military Programs. This information in the hands of Skyryse removes a large barrier to entry and saves Skyryse tens of millions of dollars and several years of work.

234. The scope of data copied by Kim and Pilkington is breathtaking in its scope and difficult to comprehend due to its vastness. They essentially copied everything that Moog's flight control software engineering teams had worked on over the fifteen (15) years up until the theft. It is impossible to quantify the amount of monetary investment, software engineering hours, and other resources that have gone into developing, testing, and certifying all of these programs and applications. This information is truly priceless and represents the highest level of intelligence and wisdom of Moog's smartest architects of the past 15 to 20 years.

235. Thousands of employees and millions of hours of work were used in

building, testing, and certifying the software and programs copied by Kim, Pilkington, and other Skyryse personnel.

236. [redacted] This software application was developed, tested, and certified through the substantial investment of training, time and money by Moog.

237. One of the notable programs copied by Kim and Pilkington is the commercial program G280, which Moog built, tested, and certified. [redacted]

238. Skyryse is now pursuing flight control systems for helicopters. The data from the G280 project is directly related to what Skyryse is pursuing and would be extremely valuable to Skyryse and would save it tremendous time, money, effort, and resources in having to build these programs from scratch.

239. As described above in detail, Skyryse is using Moog's trade secrets and other non-public information on a massive scale, including by developing its software checklists, plans, and verification criteria off of Moog's proprietary documents. These documents form the foundation for the development, testing, and certification of Skyryse's flight control software

240. It is impossible to precisely quantify the amount of monetary investment, software engineering hours, and other resources that Skyryse stands to

save by utilizing Moog's proprietary information and leveraging their former employees' knowledge to deploy that information, but the magnitude is simply massive.

241. Further, by improperly gaining access to and/or copying Platform, a third party could get easier access to perform software upgrades. Currently, only Moog can re-install or service an upgraded equipment or product which uses Platform.

242. Re-programming an airplane computer has several security concerns. A third party would not be able to pull information from an airplane box that has used certain Toolsets (including the Platform software) in order to re-program it unless it has access to Moog's software. Moreover, it potentially allows third parties to take over performing work for Moog clients that currently only Moog can perform.

243. Further, certain of the Toolsets (including Platform) have been used for several military programs. It generally takes a new hire one year to obtain sufficient access to work on military projects. Moog is not able to immediately re-allocate new employees to fill the void of its military software developers that left for Skyryse because it takes considerable time to establish required access credentials.

244. Finally, there are substantial security, goodwill, and reputational threats posed by Defendants' copying of Moog's proprietary, confidential, and trade secret software and related data. Under nearly every contract that Moog enters into for flight software development, there is a requirement that Moog notify its customers if certain proprietary or confidential data was copied or stolen. Moog has now been required to notify its customers of the data theft at issue, including the US Government. This presents a substantial distraction from normal operations and has and will require Moog to expend resources responding to government inquiries. Moog has never previously had to notify the US Government of a data theft in connection with its flight control software.

245. Moog's required disclosure poses the risk of harm to Moog's reputation and goodwill in the industry and with customers such as the US Government, which is not compensable with monetary damages. Data and information security is of paramount concern in this industry, and especially in performing work for or providing deliverables to the US Government. Moog has historically been regarded as excellent and trustworthy in terms of data security and confidentiality.

AFTER THIS LAWSUIT WAS FILED, SKYRYSE'S PRIOR COUNSEL DISCLOSES POSSESSION OF MOOG DATA AND DELETION OF DATA

246. After this lawsuit was filed, in an April 26, 2022 conference with the Court, Skyryse's prior counsel made several disclosures to Moog and the Court regarding Skyryse's possession of Moog data, deletion of data by Skyryse employees, and Skyryse placing 15 employees on administrative leave. Skyryse's prior counsel disclosed the following regarding Skyryse's possession of Moog data:

- "We have discovered that there is . . . likely, [Moog] non-public information at Skyryse";
- "we have found enough [Moog non-public information] that it does – it causes us concern";
- "We have – we appear to have non-public Moog information at Skyryse";
- Skyryse found a "significant number of hits" from the "list of file names and hash values" provided by Moog.

247. Regarding the deletion of data after this lawsuit was filed, Skyryse's prior counsel disclosed the following:

- "we have discovered forensically that since the complaint was filed certain information has been deleted";
- "What we have seen is – to us, is an alarming series of deletions";
- "it also is the case that some of the information deleted may not be recoverable";

- "that is a fact on the ground as we sit here today, unfortunately, that the information was deleted after the complaint was filed";
- "we do not have certainty it will be recoverable."

In subsequent filings, Skyryse later disclosed that its former personnel Alex Wang had deleted a number of potentially relevant files after the commencement of the lawsuit, some of which were permanently deleted and not recoverable.

248. Skyryse's prior counsel further disclosed that Kim and Pilkington had been terminated from Skyryse. Skyryse's prior counsel further disclosed that 15 Skyryse employees had been placed on administrative leave, consisting of "individuals who have been identified as having possessed Moog information, and individuals who had both evidence of deletion on their devices, and file name hits." As a result of these disclosures, Skyryse withdrew its Rule 12(b)(6) Motion to Dismiss the original Complaint.

COUNT I

Violation of the Defend Trade Secrets Act,

18 U.S.C. § 1836

(Against All Defendants)

249. Moog incorporates by reference and realleges the allegations contained in paragraphs 1 through 248 above as if fully set forth herein.

250. The DTSA forbids threatened and actual misappropriation of trade secrets "if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." 18 U.S.C. § 1836(b)(1) (as amended).

251. Under the DTSA, "trade secret" means "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing

if, (A) the owner thereof has taken reasonable measures to keep such information secret, and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information." 18 U.S.C. § 1839(3) (as amended).

252. Under the DTSA, "misappropriation" means "(A) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or (B) disclosure or use of a trade secret of another without express or implied consent by a person who: (i) used improper means to acquire knowledge of the trade secret; or (ii) at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was: (I) derived from or through a person who had used improper means to acquire the trade secret; (II) acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret; or (III) derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the use of the trade secret; or (iii) before a material change of the position of the person, knew or had reason to know that (I) the trade secret was a trade secret and (II) knowledge of the trade secret had been acquired by accident or mistake." 18 U.S.C. § 1839(5) (as amended).

253. Under the DTSA, "improper means" "(A) includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means; and (B) does not include reverse engineering, independent derivation, or any other lawful means of acquisition." 18 U.S.C. § 1839(6) (as amended).

254. Certain confidential and proprietary information of Moog constitutes trade secrets related to a product or service used in, or intended for use in, interstate commerce, including, but not limited to, the Toolsets, Programs, and other Stolen Trade Secrets described in detail above. Specifically, and as described in detail

above, the 28 trade secrets that Moog is seeking protection for under this claim are as follows:

- Software Engineering Process (Toolset)
- eRTOS (Toolset)
- Platform (Toolset)
- AMP (Toolset)
- Neo (Toolset)
- B-2 (Military Program)
- X47B (Military Program)
- TERN (Military Program)
- F15SE (Military Program)
- UCLASS (Military Program)
- F35 (Military Program)
- V280 (Military Program)
- EHFCAS (Military Program)
- Emerald (Military Program)
- Sensitive Government Program 1 (Military Program)
- Sensitive Government Program 2 (Military Program)
- Bullfrog (Military Program)
- 747-8 (Commercial Program
- 787 (Commercial Program)
- A350 (Commercial Program)
- C919 (Commercial Program)
- E2 (Commercial Program)
- G280 (Commercial Program)
- G650, G700, and G800 (Commercial Programs)
- Cost Estimating Templates
- Autopilot Program

- Proposal Data
- Reid Raithel – trade secret documents stolen from Moog in coordination with Skyryse

255. Moog derives economic value from the fact that its trade secrets and confidential and proprietary information, such as the Stolen Trade Secrets, are not generally known to individuals or entities outside of Moog.

256. Moog takes reasonable measures to protect the secrecy of such trade secrets and confidential and proprietary information. These measures include, among other things, that: (1) the Stolen Trade Secrets are housed on a secure server at Moog and only certain employees at Moog have access to the software database on a "need to know" basis that must be approved by the lead on the software program; (2) five separate sets of credentials are required to access Moog's software database; (3) the Stolen Trade Secrets as applied to military projects requires elevated access credentials by the US Government; (4) the software used in the Toolsets and Programs are designed to prevent hacking or reverse engineering, and cannot be reverse engineered from an aircraft computer that has used the software; (5) Moog has controlled access into its buildings, and all employees must undergo security screening and background check before being hired; (6) Moog requires its employees to review its employee handbook (which has detailed policies about Moog's confidential and proprietary information, and a prohibition on disclosing or copying such information), acknowledge its receipt, and agree to abide by its policies; (7) Moog has robust written policies regarding its proprietary and trade secret information, and requires its software engineers to complete a training regarding company trade secrets and other proprietary information to confirm such policies; (8) Moog requires its departing employees to sign an exit form which affirms that they have been granted access to Moog's proprietary information, that they no longer have any access or copies of such materials, and that they will not breach their fiduciary duties to Moog or usurp any corporate opportunity; (9) all

Moog flight software source code files are designated as proprietary and confidential and prohibit disclosure; and (10) Moog enters into NDAs with parties where confidential and proprietary information may be disclosed on a limited basis, and in fact entered into multiple NDAs with Skyryse in the past, as explained above.

257. Both Pilkington and Kim, and the other former Moog and subsequent Skyryse employees addressed herein, knew they each had a duty to maintain the secrecy of Moog's trade secrets and confidential and proprietary information due, in part, to their fiduciary duty and duty of loyalty to Moog.

258. Aware of the secrecy and value of Moog's trade secrets and confidential and proprietary information, on information and belief, Skyryse nevertheless coordinated with Pilkington and Kim and the other Skyryse personnel identified above in efforts to misappropriate such material of and from Moog. Having signed multiple NDAs with Moog in the past, Skyryse was under an additional contractual duty not to violate those NDAs, including by disclosure and use of Skyryse's confidential and proprietary material.

259. Moreover, having worked with Moog in the past, Skyryse and its C-suite level employees, Messrs. Baptist and Rey were well aware of the value Moog placed on its trade secrets and confidential and proprietary information. Skyryse clearly appreciated how valuable it is – Skyryse originally approached Moog as a business partner because it wanted to use Platform in its own product.

260. Further, Skyryse is under a duty to not accept any misappropriated trade secrets and confidential and proprietary information, including Moog's trade secrets and confidential and proprietary information, and Skyryse is also under a duty not to disclose or use misappropriated trade secrets and confidential and proprietary information for the purpose of gaining a competitive advantage in the marketplace.

261. Defendants misappropriated Moog's trade secrets and confidential and proprietary information. In coordination with Skyryse, Kim, Pilkington, and other

Skyryse personnel copied and delivered to Skyryse the substantial volume of data files that were copied from Moog containing Moog's trade secrets and confidential and proprietary information for Skyryse's use in, in connection with, and for the advancement of Skyryse's business. As described above in detail, Skyryse has in fact used Moog's trade secrets in connection with the development, testing, and certification of Skyryse's flight control software. Therefore, Defendants have already willfully and maliciously acquired, disclosed, and used Moog's trade secrets and confidential and proprietary information without consent of any kind for their own financial gain. And Defendants will continue to do so if not enjoined by this Court.

262. On information and belief, Defendants will continue to disclose and utilize Moog's trade secrets and confidential and proprietary information by using this information to unfairly compete with Moog by improperly using that information in its own development projects and to aid soliciting business for Skyryse.

263. Indeed, as a result of Defendants' collective actions, Skyryse now has Moog's trade secret, confidential, and proprietary information as a result of the theft from Moog of approximately 1.4 million files, which Skyryse can use and is using to its competitive advantage.

264. The actions of Defendants constitute actual or threatened misappropriation under the DTSA.

265. Moog has suffered damages as a result of Defendants' actual and/or threatened breach of the DTSA, including the ongoing loss of employees, harm to its goodwill and reputation, and an unfair reduction in its competitive advantage.

266. Moog is entitled to actual damages from Defendants, jointly and severally, to exemplary damages pursuant to 18 U.S.C. § 1836(b)(3)(C), and to attorneys' fees pursuant to 18 U.S.C. § 1836(b)(3)(D).

267. Moog's damages cannot be adequately compensated through remedies

at law alone, thereby requiring equitable relief in addition to compensatory relief.

268. Defendants' actions will continue to cause irreparable harm and damages to Moog and its trade secrets and confidential and proprietary information if not restrained.

COUNT II

CONVERSION

(Against All Defendants)

269. Moog incorporates by reference and realleges the allegations contained in paragraphs 1 through 268 above as if fully set forth herein.

270. Moog owns and possesses, and at all relevant times has owned and possessed, the Stolen Non-Trade Secret Data.

271. Defendants, and each of them, have substantially interfered with Moog's property by knowingly or intentionally taking possession of the Stolen Non-Trade Secret Data, as well as using them and disclosing them to third parties.

272. Moog did not consent to Defendants' possession, use, or disclosure of the Stolen Non-Trade Secret Data.

273. Defendants' conduct is, and has been, a substantial factor in causing Moog harm.

274. Defendants' unlawful and unauthorized possession, use, and disclosure of the Stolen Non-Trade Secret Data has and will directly and proximately cause Moog to suffer great damage and injury, and Moog will continue to suffer damage by the continued acts of Defendants in an amount to be proven at trial.

COUNT III

BREACH OF FIDUCIARY DUTY AND DUTY OF LOYALTY

(Against Pilkington and Kim)

275. Moog incorporates by reference and realleges the allegations contained in paragraphs 1 through 274 above as if fully set forth herein.

276. By virtue of Pilkington's and Kim's employment relationship with

Moog, including assignment to sensitive programs requiring additional vetting and commitment to the protection of such information from misuse, Moog reposed trust and confidence in each of Pilkington and Kim to provide services and perform their duties, and to refrain from acting in any manner contrary to Moog's interests.

277. Pilkington and Kim each undertook such trust and confidence.

278. By reason of the foregoing, Pilkington and Kim each owed Moog a fiduciary duty and duty of loyalty to act in good faith and in Moog's best interest, which includes a duty not to disclose or use the employer's proprietary or confidential information for the purpose of competing with their employer or for his or her own personal gain. These duties were confirmed and agreed in writing in at least Kim's Exit Form, which she signed on December 17, 2021.

279. Such fiduciary duty and duty of loyalty owed by Pilkington and Kim to Moog existed throughout their respective employments with Moog and survived the termination of that employment.

280. Pilkington and Kim breached their fiduciary duty and duty of loyalty to Moog by engaging in the wrongful activity as described herein, including but not limited to, the theft of vast swaths of the Stolen Trade Secrets and Stolen Non-Trade Secret Data, and misappropriation of Moog's trade secrets and confidential and proprietary information for their benefit and the benefit of Skyryse, a competitor of Moog, and by scheming to solicit away employees of Moog while still employed by Moog.

281. Pilkington's and Kim's actions were and are willful and malicious and without legal justification or excuse.

282. Pilkington's and Kim's breach of their fiduciary duty of loyalty has and will continue to directly and proximately cause substantial damage to Moog and its business, including damage to its reputation.

283. Pilkington's and Kim's breach of their fiduciary duty of loyalty has directly and proximately caused Moog to suffer great damage and injury, and Moog

will continue to suffer damage and injury by the continued acts of Pilkington and Kim.

COUNT IV

AIDING AND ABETTING BREACH OF FIDUCIARY DUTY

(Against Pilkington and Kim)

284. Moog incorporates by reference and realleges the allegations contained in paragraphs 1 through 283 above as if fully set forth herein.

285. Pilkington aided and abetted Kim's breach of fiduciary duty by collaborating with her to misappropriate Moog's trade secrets and confidential and proprietary information, and by contributing to and encouraging her tortious activity.

286. Kim aided and abetted Pilkington's breach of fiduciary duty by collaborating with him to misappropriate Moog's data and confidential and proprietary information, and by contributing to and encouraging his tortious activity.

287. Upon information and belief, Kim and Pilkington conspired and reached an agreement to steal and misappropriate Moog's data and confidential and proprietary information for their benefit and use at Skyryse.

288. On information and belief, Pilkington had actual knowledge of Kim's breach of fiduciary duty, as he knew that she was providing him and Skyryse with Moog's property (including proprietary and confidential files) that she stole from Moog in furtherance of her own self-interest and in furtherance of the interests of Pilkington and Skyryse. Pilkington provided substantial assistance by collaborating with Kim to misappropriate and steal what they knew to be Moog's confidential, proprietary, and trade secret information. Indeed, upon information and belief, Pilkington directed Kim to use Pilkington's file path in copying Moog's data. Pilkington aided and abetted Kim's breach of fiduciary duty intentionally and without justification.

289. On information and belief, Kim had actual knowledge of Pilkington's

breach of fiduciary duty, as she knew that he was providing her and Skyryse with Moog's property (including proprietary and confidential files) in furtherance of his own self-interest and in furtherance of the interests of Kim and Skyryse. Kim provided substantial assistance by collaborating with Pilkington to misappropriate and steal what they knew to be Moog's confidential, proprietary, and trade secret information. Indeed, both Kim and Pilkington plugged in Samsung 2 Hard Drive into their respective Moog computers at the same time before their departure from Moog, and which Pilkington used to copy massive amounts of Moog data to the hard drive. Kim aided and abetted Pilkington's breach of fiduciary duty intentionally and without justification.

290. The participation of Pilkington in the breach of Kim's fiduciary duties has and will directly and proximately cause substantial damage to Moog and its business, including damage to its reputation.

291. The participation of Kim in the breach of Pilkington's fiduciary duties has and will directly and proximately cause substantial damage to Moog and its business, including damage to its reputation.

292. The participation of Kim in the breach of Pilkington's fiduciary duties has directly and proximately caused Moog to suffer great damage and injury, and Moog will continue to suffer damage by the continued acts of Pilkington.

293. The participation of Pilkington in the breach of Kim's fiduciary duties has directly and proximately caused Moog to suffer great damage and injury, and Moog will continue to suffer damage by the continued acts of Kim.

COUNT V

CONSPIRACY

(Against All Defendants)

294. Moog incorporates by reference and realleges the allegations contained in paragraphs 1 through 293 above as if fully set forth herein.

295. As alleged herein, Defendants committed the underlying tort of

misappropriation and theft of the Stolen Trade Secrets, as well as conversion of the Stolen Non-Trade Secret Data.

296. On information and belief, each of the Defendants reached an agreement to commit the above alleged torts. This agreement is indicated by their collaboration and cooperation to use Moog's trade secret, confidential and proprietary information in and for Skyryse's business. Specifically, this agreement is shown through: a) the sheer number of Skyryse personnel (at least 22 in total) directly implicated in the possession, use, and disclosure of the Stolen Trade Secrets and Stolen Non-Trade Secret Data, including high level employees (such as Sathya Achar); b) the pervasive use of the Stolen Trade Secrets and Stolen Non-Trade Secret Data in connection with Skyryse's flight control software plans, testing, and certification (which directly overlapped with the hardware and services that Moog provided to Skyryse under SOW1); and 3) the collaboration overlap between the separate acts of theft and misappropriation of the Stolen Trade Secrets and Stolen Non-Trade Secret Data amongst Pilkington and Kim, including Kim's use of Pilkington's file path, and their use of common devices to further their wrongful acts.

297. As alleged in detail herein, each of the Defendants committed an act in furtherance of the agreement to commit the above alleged torts, as indicated by their collaboration and cooperation to use Moog's trade secret, confidential and proprietary information in and for Skyryse's business. Gonzalo Rey and Sathya Achar were also involved in, and key orchestrators of, the conspiracy alleged herein. Rey, an executive at Moog who pioneered the development of its flight control software, was the first Moog employee to join Skyryse. On information and belief, he is now a high-level executive at Skyryse pursuing the development of a competing flight control software, and he has been the lead individual involved in Skyryse's targeted solicitation of Moog's software engineers. Sathyanarayana Achar (former Engineering Technical Fellow) was one of the first Moog employees to

sponsor and oversee the development of Moog's Toolsets (including the Platform base software) beginning in 2007. He has the most institutional and technical knowledge regarding the Toolsets, as well as its relationship with project-specific applications which sit on top of the Toolsets. He is also familiar with the Moog personnel who developed the Toolsets. On information and belief, Achar is now a Vice President at Skyryse.

298. The current and former Skyryse personnel involved in the conspiracy, and who each committed acts in furtherance of the agreement to commit the above alleged torts, are several and voluminous. They include at least, as alleged in detail above, Gonzalo Rey, Tim Baptist, Sathya Achar, Eric Chung, Reid Raithel, Lori Bird, Tri Dao, Alex Wang, Amir Hallajpour, Chris Smith, David Lee, Diane Li, Hussein Khimji, Ian Young, Lawrence Chow, Mario Brenes, Norman Butler, Paul Kapaun, Stephen Wang, Ilan Paz, Thusa Dinh, and Glenn Shintaku.

299. Defendants' conspiracy to commit the above alleged tort has and will directly and proximately cause substantial damage to Moog and its business, including the loss of market share and prospective customers, loss of its trade secrets and confidential and proprietary information, and damage to its reputation.

300. Defendants' conspiracy to commit the above alleged tort has and will directly and proximately cause Moog to suffer great damage and injury, and Moog will continue to suffer damage by the continued acts of Defendants.

COUNT VI

BREACH OF CONTRACT

(Against Skyryse)

301. Moog incorporates by reference and realleges the allegations contained in paragraphs 1 through 300 above as if fully set forth herein.

302. As explained above, on October 24, 2018, Moog and Skyryse entered into the 2018 NDA, and, on March 15, 2019, Moog and Skyryse entered into the 2019 NDA.

303. Section 2 of the 2018 and 2019 NDAs provides: "Neither Party shall disclose, in whole or in part, by any means whatsoever, any Proprietary Information provided by the disclosing Party to any third party without the express prior written consent of the disclosing Party. The receiving Party shall not alter, modify, decompile, disassemble, reverse engineer, translate or create derivative works from the disclosing Party's Proprietary Information. The receiving Party shall use Proprietary Information of the disclosing Party only for the limited purpose described above and not for any other purpose."

304. Section 3 of the 2018 and 2019 NDAs provides: "Each Party shall utilize the same degree of care to preserve and protect the other Party's Proprietary Information from disclosure, and otherwise limit access, as it uses to protect its own Proprietary Information, which degree of care will not be less than reasonable care."

305. Section 5 of the NDAs confirms the effective term for both agreements is ten years for the execution date.

306. Section 8 of the NDAs provides: "A breach of any of the terms of this Agreement will result in irreparable and continuing damage for which there may be no adequate remedy at law and the non-breaching Party shall be entitled to seek injunctive relief, without the necessity of posting a bond, and such other relief, including monetary damages, if appropriate, against the breaching Party and/or any other person or entity liable for the unauthorized or wrongful use or disclosure of Proprietary Information received hereunder."

307. Moog did all of the significant things that the 2018 and 2019 NDAs required it to do. Moog complied with the 2018 and 2019 NDAs.

308. In breach of the 2018 NDA and 2019 NDA, Skyryse used information gained from Moog regarding its flight control software between 2018-2020 during the Parties' business relationship for purposes beyond the scope of the limited purpose of the Parties' business engagement in Phase 1 under the SOW, including to: 1) develop its own flight control systems and software; and 2) raid and solicit

Moog's key software engineering personnel who have most knowledge of Moog's flight control software. Upon information and belief, Skyryse attempted to or in fact did reverse engineer certain components of Moog's flight control systems disclosed to Skyryse between 2018-2020 in an effort to develop a competing flight control system, which is expressly prohibited under the 2018 and 2019 NDAs. Skyryse used confidential information provided by Moog under the 2018 and 2019 NDAs regarding Moog's software engineering staff and technology to engage in targeted hiring and data theft practices a few years later. Moog's breach of contract claim against Skyryse is predicated on Skyryse's unlawful and unauthorized use of information, software, and hardware that Moog disclosed to Skyryse between 2018-2020 and under the protections of the 2018 and 2019 NDAs.

309. Skyryse's breaches of the 2018 NDA and 2019 NDA directly and proximately caused and continue to cause Moog to suffer great damage and injury, and Moog will continue to suffer damage as a result of Skyryse's ongoing breaches of the 2018 NDA and 2019 NDA.

COUNT VII

BREACH OF CONTRACT

(Against Pilkington and Kim)

310. Moog incorporates by reference and realleges the allegations contained in paragraphs 1 through 309 above as if fully set forth herein.

311. Pilkington acknowledged his receipt of the Employee Handbook and agreed to abide by its policies on July 30, 2012. Kim acknowledged her receipt and agreed to abide by its policies on January 21, 2013.

312. On Page 58, the Employee Handbook provides: "Unless acting in the proper performance of your duties, or required by law, you must not disclose to any person or body, including work colleagues, or use any confidential information that you obtain during the course of your employment. These restrictions will continue after your employment has been terminated."

313. On Page 59, the Employee Handbook provides: "Confidential information belonging to the company will remain the property of the company and you must not retain any copies of this information . . . Any breach of confidentiality, including the imparting of information to other employees, except on a ''need to know' basis, will be considered grounds for summary dismissal and breach of contract for which damages may be claimed."

314. Pilkington and Kim breached the terms of Moog's Employee Handbook by engaging in the wrongful activity as described herein, including but not limited to, the misappropriation of Moog's trade secrets and confidential and proprietary information for their benefit and the benefit of Skyryse, a competitor of Moog, and by scheming to solicit away employees of Moog while still employed by Moog.

315. Further, Kim signed the Exit Form on her last date of employment at Moog on December 17, 2021.

316. In the Exit Form, Kim agreed that she had returned all Moog "TRADE SECRET/COMPANY CONFIDENTIAL INFO." The Exit Form also provides, among other things: 1) Kim "owes a fiduciary duty to Moog to not usurp any such corporate opportunity for [her] own benefit"; and 2) Kim affirms that she does "not maintain access to, or have possession of, any tangible or digital record of Moog IP—whether in hard copy or digital form—on any device, cloud, or digital storage facilities."

317. Kim breached her obligations under the Exit Form because she: 1) copied over 136,000 files of confidential and proprietary Moog data and kept it with her after her employment ended; 2) deleted the Moog data she copied on the external hard drive she used; and 3) breached her fiduciary duties to Moog by usurping Moog's corporate opportunities to the benefit of herself, Pilkington, and Skyryse.

318. Pilkington's and Kim's respective breaches of said agreements directly

and proximately caused and continue to cause Moog to suffer great damage and injury, and Moog will continue to suffer damage as a result of Pilkington's and Kim's respective ongoing breaches of those agreements.

COUNT IX

BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

(Against Skyryse)

319. Moog incorporates by reference and realleges the allegations contained in paragraphs 1 through 318 above as if fully set forth herein.

320. In every contract or agreement there is an implied promise of good faith and fair dealing. This implied promise means that each party will not do anything to unfairly interfere with the right of any other party to receive the benefits of the contract. Good faith means honesty of purpose without any intention to mislead or to take unfair advantage of another.

321. As explained above, on October 24, 2018, Moog and Skyryse entered into the 2018 NDA, and, on March 15, 2019, Moog and Skyryse entered into the 2019 NDA.

322. Moog did all of the significant things that the 2018 and 2019 NDAs required it to do. Moog complied with the 2018 and 2019 NDAs.

323. All conditions for Skyryse's performance under the 2018 and 2019 NDAs were met.

324. The 2018 and 2019 NDAs were all subject to an implied covenant of good faith and fair dealing that Skyryse would act in good faith and with reasonable efforts to perform its contractual duties and to not impair Moog's rights to receive its rights, benefits, and reasonable expectations under the 2018 and 2019 NDAs.

325. Skyryse prevented Moog from receiving the benefits of the 2018 and 2019 NDAs by, as alleged in further detail above: 1) hiring dozens of key, targeted Moog personnel after the NDAs were entered into who have intimate knowledge

about the confidential information that Moog disclosed to Skyryse under the 2018 and 2019 NDAs; 2) having its employees steal approximately 1.4 million files from Moog without authorization, which include hundreds of thousands of files reflecting Moog's trade secrets; and 3) using the Stolen Trade Secrets and Stolen Non-Trade Secret Data in connection with the development, certification, and testing of Skyryse's flight control software and programs. Moog's breach of the implied covenant claim is predicated on the hiring of dozens of Moog employees to circumvent the protections under the 2018 and 2019 NDAs, as well as Skyryse's theft and use of the Stolen Trade Secrets and Solen Non-Trade Secret Data between 2021-2022 after the Parties' business relationship ended.

326. As a result of its conduct, Skyryse did not act fairly and in good faith, and deprived Moog of the full benefit of the parties' bargains under the 2018 and 2019 NDAs.

327. Moog was been harmed by Skyryse's breaches of the covenants of good faith and fair dealing and is entitled to damages in an amount to be proven at trial.

COUNT X

UNJUST ENRICHMENT

(Against All Defendants)

328. Moog incorporates by reference and realleges the allegations contained in paragraphs 1 through 327 above as if fully set forth herein.

329. Defendants have unjustly received and retained the benefits of the efforts and investments of Moog to the detriment of Moog.

330. Defendants have unjustly and improperly utilized to their benefit the Moog's effort and investment in a host of employees raided by Defendants and in confidential and proprietary information developed by Moog, to the benefit of Skyryse's business and the advantage of Pilkington and Kim. Skyryse has used the Stolen Trade Secrets and Stolen Non-Trade Secret Data in connection with the

development, certification, and testing of Skyryse's flight control software and programs, thereby saving Skyryse several years and many millions of dollars that it would ordinarily take to develop this information and technology on its own.

331. Kim and Pilkington were specifically unjustly enriched through their conduct because their theft and misappropriation of the Stolen Trade Secrets and Stolen Non-Trade Secret Data allowed Kim and Pilkington to obtain benefits in their employment at Skyryse. These benefits include, upon information and belief, higher salaries, benefits, or other compensation, increased responsibility and advancement at Skyryse, and the ability to quickly build software and programs at Skyryse that ordinarily would take a much longer time to develop without the use of Moog's data.

332. Defendants have been unjustly enriched, and it is against equity and good conscience to permit Defendants to retain the benefits of the efforts and investments of Moog.

333. Moog has no adequate remedy at law.

COUNT XI

IMPOSITION OF CONSTRUCTIVE TRUST

(Against All Defendants)

334. Moog incorporates by reference and realleges the allegations contained in paragraphs 1 through 333 above as if fully set forth herein.

335. At all times during their employment at Moog, and continuing after their employment, Pilkington and Kim owed fiduciary duties of loyalty and care to Moog. These duties, including obligations not to misappropriate or disclose Moog's proprietary and trade secret information, were further confirmed in Moog's trade secret trainings, the Exit Form, Moog's designations on its source code documents, and elsewhere.

336. During their employment, Pilkington and Kim promised not to misappropriate, misuse, or otherwise disclose Moog's confidential, proprietary, and

trade secret information, and to not usurp a corporate opportunity of Moog.

337. In reliance on these promises, Moog granted access credentials to Pilkington and Kim to Moog's most confidential, proprietary, and trade secret information. Pilkington and Kim knew that they were only allowed to access these programs for legitimate business purposes of Moog. As described above, Pilkington and Kim used this position of trust and confidence to orchestrate a scheme to copy and steal approximately 1.4 million files from Moog around the time Kim and Pilkington left Moog to join Skyryse.

338. Similarly, Moog and Skyryse entered into a confidential relationship as evidenced by the 2018 and 2019 NDAs, which expressly prohibited use of confidential information disclosed thereunder beyond the scope of the Parties' contemplated business arrangement at the time.

339. Skyryse therefore promised not to use Moog's confidential and trade secret information for its own gain beyond the scope of the NDAs. In reliance on that promise, Moog provided considerable confidential information under the NDAs, including certain information related to its flight control systems and software functionalities.

340. As alleged above, Skyryse used the confidential information that Moog provided under the NDAs in an improper manner, including to develop its own competing flight control systems and software, and to raid and solicit Moog's most knowledgeable employees regarding its flight control software.

341. Defendants, and each of them, have been unjustly enriched by the confidential, proprietary, and trade secret information that they have improperly used and stolen from Moog. Skyryse is using the Stolen Trade Secrets and Stolen Non-Trade Secret Data to develop its own competing flight control software to the direct harm of Moog.

342. Moog has no remedy at law to address this misconduct. Defendants are in possession of a large volume of Moog data and information of which they have

no right to possess. It is just and equitable that this Court impose a constructive trust to attach on all of Moog's confidential information and data that Defendants, and each of them, improperly took and from the time it entered their possession.

COUNT XII

VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW (BUS. & PROF. CODE § 17200, ET SEQ.)

(Against Skyryse)

343. Moog incorporates by reference and realleges the allegations contained in paragraphs 1 through 342 above as if fully set forth herein.

344. California's Unfair Competition Law prohibits unlawful, unfair, or fraudulent conduct.

345. Skyryse's conduct is unlawful based on the wrongful conduct and other causes of action alleged herein.

346. Skyryse has also, in bad faith, employed unfair means, including but not limited to inducing Pilkington and Kim to: violate their duties of loyalty to Moog; lure away key software development employees from Moog; and misappropriate and use Moog's trade secret, confidential, and proprietary information, as part of a deliberate and malicious strategy to harm Moog's business and unfairly trade on Moog's investments of time and money in software and employees.

347. To date, Skyryse has successfully raided 20 Moog employees, including high-level Moog officers, senior level engineers, coding engineers, and testers, and has reached out to many software engineers at Moog who worked on Moog projects intersecting with the Stolen Trade Secrets and Stolen Non-Trade Secret Data in the United States, specifically targeting Moog's Los Angeles-area office.

348. Replacing these lost employees has impacted work production due to the elevated access credentials needed to support the Sensitive Government

Programs.

349. Skyryse has raided these employees as part of its scheme to gain access to confidential, proprietary trade secret information, including but not limited to the Toolsets and Programs. In concert with several former Moog employees, including Pilkington and Kim, Skyryse has improperly and wrongfully acquired this information.

350. Skyryse misappropriated Moog's trade secrets and confidential and proprietary information on its own and in coordination with Pilkington, Kim, and several other former Moog employees.

351. Skyryse has used and continues to use Moog's trade secrets and confidential and proprietary information to gain a competitive advantage over Moog (and other competitors) in the flight control software market.

352. Skyryse has no legitimate business justification for its actions and such actions were done in bad faith and with the intent to harm Moog.

353. Unmanned helicopter aviation, which Moog is pursuing and understands Skyryse is also pursuing, is a new market. There is no established market and no industry leader yet. About twenty (20) companies, including Moog and Skyryse, have entered the market and are rushing to become the market leader. Whichever company wins that race will likely win a large portion of the market share just by being the first to market with a viable product. If another party gained access to the Stolen Trade Secrets and Stolen Non-Trade Secret Data, it would give that party a substantial and unfair competitive advantage as it would save that party many millions of dollars and many years investing in development and testing that software. Moog has invested approximately eleven (11) years of research and development into automated flight technologies and sixteen (16) years in developing the Stolen Trade Secrets. As noted, the Toolsets, Programs, and other Stolen Trade Secrets take many years to build, test, and certify. By stealing Moog's source code and other proprietary information underlying the Toolsets and Programs, and

crippling Moog's software engineering workforce, Skyryse has jumped to the front of this race to be first to market and has slashed Moog's tires along the way.

354. Skyryse's actions are unfair because they have harmed competition in the highly-competitive industry of unmanned helicopter aviation. This is a new market with no established industry leader yet. By getting a close look under the hood of Moog's flight control technologies in between 2018 and 2020, and then subsequently pivoting its business and hiring a large portion of Moog's entire software engineering team, Skyryse has harmed competition in general in the unmanned helicopter aviation industry. Even setting aside the theft of the Stolen Trade Secrets and Stolen Non-Trade Secret Data, Skyryse has also effectively stolen Moog's intellectual property by hiring a majority of its flight control software engineers.

355. Skyryse's unfair competition has and will directly and proximately cause substantial damage to Moog and its business, including the loss of market share and prospective customers, loss of its trade secrets and confidential and proprietary information, and damage to its reputation.

356. Skyryse's acts of unfair competition have and will directly and proximately cause Moog to suffer great damage and injury, and Moog will continue to suffer damage by the continued acts of Skyryse.

WHEREFORE, Moog demands judgment against Defendants as follows:

(1) For a permanent injunction enjoining Defendants and their agents, servants, employees, officers, attorneys, successors, licensees, partners, and assigns, and all other persons acting in concert with them from:

(a) directly or indirectly using, accessing, disclosing, copying, or transmitting, for any purpose, any non-public information, documents, records, files, or data in any Defendant's possession, custody, or control (i) of, from, or belonging to Moog, (ii) provided, offered, transmitted, or conveyed to any Defendant by

any current or former Moog employee, and/or (iii) copied or taken from Moog's computers, servers, databases, networks, or systems, including without limitation any and all information, documents, files, or data copied or downloaded by Kim and/or Pilkington from Moog's computers, servers, databases, or systems, regardless of the medium on which such materials were copied, transferred, or stored;

(b) directly or indirectly soliciting, influencing, inducing, recruiting or causing any Moog employee in Moog's aircraft flight control business to terminate his or her employment for the purpose of joining, associating or becoming employed with Skyryse;

(c) continuing to possess or use Moog's confidential, proprietary, and/or and trade secret information;

(d) preserving and turning over all evidence of any non-public information, documents, records, files, or data in any Defendant's possession, custody, or control belonging to Moog; and

(e) such other relief as the Court may deem appropriate as against Defendants;

(2) For an award of Moog's actual damages and lost profits it has sustained as a result of Defendants' unlawful acts of misappropriation of Moog's trade secrets and confidential information, and to recover from Defendants' the gains, profits, and advantages Defendants have obtained as a result of the wrongful conduct alleged herein, in an amount to be determined at trial;

(3) For an order awarding Moog its attorneys' fees under the Defend Trade Secrets Act 18 U.S.C. § 1836(b)(3)(D);

(4) For an imposition of a constructive trust on the information and data that Defendants wrongfully took from Moog and held by Defendants (and any

profits derived therefrom), and order that such information be held for Moog's benefit and transferred in full to Moog;

(5) For an order awarding Moog exemplary damages in an amount twice the amount of actual damages awarded, for willful and malicious misappropriation under the Defend Trade Secrets Act pursuant to 18 U.S.C. § 1836(b)(3)(D);

(6) For an order awarding Moog all costs, litigation expenses, and actual, reasonable attorneys' fees pursuant to the breached contracts;

(7) For an award of compensatory damages against Defendants in favor of Moog;

(8) For an award of punitive damages against Defendants and in favor of Moog;

(9) For an order that Moog recover its costs from Defendants;

(10) For prejudgment and post judgment interest; and

(11) For such other and further relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Moog demands a trial by jury of all issues so triable.

Dated: Julv 21. 2023

SHEPPARD MULLIN RICHTER & HAMPTON LLP

By *<u>/s/ Kazim A. Naqvi</u>*
Kazim A. Naqvi

Attorney for Plaintiff and Counterdefendant MOOG INC.